EnGenius®

Business Solutions

User Manual

EWS5912FP | EWS7928P | EWS7952FP

version 1.0

Wireless Management Switch

Neutron Series

IMPORTANT

To install your Switch please refer to the
Quick Installation Guide included in the product packaging.

Table of Contents

Chapter 1 Product Overview..... 7
Introduction/Package Contents..... 8
Technical Specifications..... 9
Physical Interface..... 12
Compatibility..... 14
Management Interface..... 15
Connecting the Switch to a Network..... 16
Web Access..... 18
Chapter 2 Controller Management..... 19
- Wireless Controller & L2 Switch..... 20
Device Management..... 21
- Summary..... 21
- Access Points..... 22
- General/Global Settings..... 25
- Autoconfiguration..... 25
- How to Add Access Points to an Access Point List... 27
- Individual Access Points Settings..... 28
- Wireless Radio Settings 2.4 GHz/5 GHz..... 29
- WLAN Settings 2.4 GHz/5 GHz..... 32
- SSID Configuration..... 33
- Basic..... 33
- Traffic Shaping..... 33
- Fast Roaming..... 33
- Security/WEP..... 34
- WPA2/WPA2 Enterprise..... 35
- WPA-PSK/WPA2-PSK..... 35
- Advanced Settings..... 36
- Guest Network..... 37
- Security..... 37
- Manual IP Settings & Auto DHCP Server Settings..... 37
- Active Clients..... 39
- Access Point Clusters..... 41
- General/Global Settings..... 42
- Member Settings/Autoconfiguration..... 43
- Radio Settings - 2.4 GHz/5 GHz..... 43
- Autoconfiguration..... 43
- Wireless Radio Settings 2.4 GHz/5 GHz..... 44
- Advanced Settings..... 46
Visual Monitoring..... 48
- Topology View..... 48
- Navigation Tips..... 49
- Map View..... 50
- Navigation Tips..... 51
- Floor View/Floorplan Image..... 52
- Status Dashboard..... 53
- Managing Images..... 53
- Floorplan View/Floor View..... 53
- Navigation Tips/Color Legend..... 54
- How to use a Floor Plan View..... 54
Statistics..... 55
- Access Points..... 55
- Wireless Clients..... 57
Maintenance 59
- SSL Certificate..... 59
- Generating a New Certificate..... 59
- Certification Information..... 60
- Advanced Options..... 60

- Trouble Shooting..... 61
- Choosing an Access Point to Diagnose..... 61
- Bulk Upgrade..... 63
- Device List 63

Chapter 3 Switch Management..... 65

System..... 66
- Summary..... 67
- Search Bar..... 67
- IP Settings..... 68
- IPv4..... 68
- IPv6..... 70
- System Time..... 71
- Port Settings..... 73
- PoE 75
- Power Budget..... 75
- PoE Port Settings..... 76
- EEE..... 79

L2 Features..... 80
- Link Aggregation..... 80
- Port Trunking 82
- Dynamic LACP..... 83
- LACP Settings..... 84
- LACP Timout..... 85
- Mirror Settings..... 86
- STP..... 88
- Global Settings..... 88
- Spanning Tree Loops..... 89
- Root Bridge..... 91
- Port Settings..... 93
- Edge Ports..... 94
- CIST Instance Settings..... 95
- CIST Port Settings..... 97
- MST Instance Settings..... 99
- MST Port Settings..... 102
- MAC Address Table..... 104
- Static MAC Address..... 104
- Dynamic MAC Address..... 105
- LLDP..... 106
- Global Settings..... 107
- Local Device..... 108
- Remote Device..... 109
- IGMP Snooping..... 111
- Global Settings..... 112
- VLAN Settings..... 113
- Querier Settings..... 114
- Group List..... 116
- Router Settings..... 117
- MLD Snooping..... 118
- Global Settings..... 118
- VLAN Settings..... 119
- Group List..... 120
- Router Settings..... 121
- Jumbo Frame 122

VLAN..... 123
- 802.1Q..... 123
- PVID..... 126
- Management VLAN..... 128
- Voice VLAN..... 129

- Global Settings.....129
- OUI Settings.....130
- Port Settings.....131
Management.....132
- System Info.....132
- User Management.....133
- File Management.....134
- Configuration Manager.....134
- Dual Image.....135
- SNMP.....136
- Global Settings.....138
- View List.....139
- Group List.....140
- Community List.....141
- User List.....142
-Trap Settings/SNMP Traps.....143
ACL.....145
- MAC ACL.....146
- MAC ACE.....147
- IPv4 ACL.....148
- IPv4 ACE.....149
- IPv6 ACL.....151
- IPv6 ACE.....152
- ACL Binding.....154
QoS.....155
- Global Settings.....155
- CoS Mapping.....157
- DSCP Mapping.....158
- Port Settings.....159
- Bandwidth Control.....160
- Storm Control.....161
Security.....162
- 802.1X.....162
- Global Settings.....163
- Port Settings.....164
- Authenticated Host.....166
- Radius Server.....167
- Access.....169
- HTTP(S) Settings.....169
- Telnet Settings.....170
- SSH Settings.....171
- Console Settings.....172
- Port Security.....173
- DoS.....174
- Global Settings.....174
- Port Settings.....176
Monitoring.....177
- Port Statistics.....177
- RMON.....178
- Event List.....178
- Event Log Table.....179
- Alarm List.....180
- History List.....181
- History Log Table.....182
- Statistics.....183
- Log.....184
- Global Settings.....185
- Local Logging.....186

- Remote Logging..... 188
- Log Table..... 189
Diagnostics..... 190
- Cable Diagnostics.....190
- Ping Test..... 191
- Ping Test Settings..... 191
- IPv6 Ping Test..... 192
- Trace Route..... 193

Chapter 4 Maintenance.....194

Maintenance..... 195
Upgrading/Resetting..... 196
Rebooting/Logging Out..... 197

Appendix..... 198

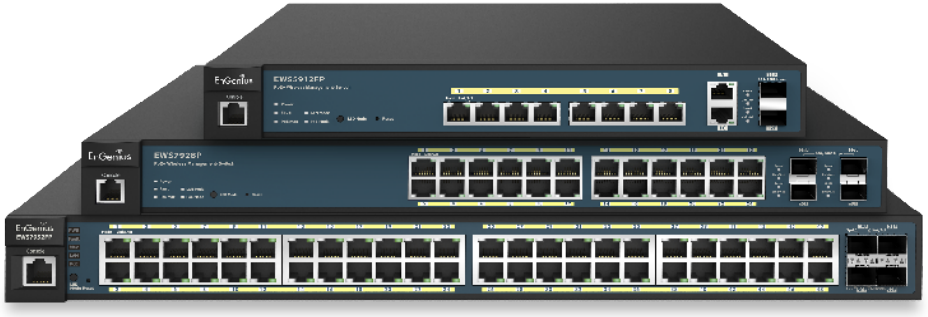
Quick Reference Guide..... 199
Professional Installation Instruction (English/French). 200
FCC Interference Statement..... 202
IC Interference Statement..... 203
CE Interference Statement..... 205

Chapter 1

Product Overview

Introduction

The EnGenius Neutron Series of EWS PoE+ Switches/ Controllers are devices specially designed to support Access Points and IP Surveillance cameras, Voice over IP (VOIP) phones, and other Power over Ethernet (PoE)-Capable devices as well as other Ethernet-based networking equipment or computers.The EWS Layer 2 PoE+ Switch provides simple, yet powerful PoE manageability with features such as: IEEE 802.3af or IEEE 802.3at/af ports, PoE port management, loopback detection, and IGMP snooping.



Package Contents

Your EnGenius EWS Switch package will contain the following items:*

- EnGenius Switch
- Power Cord
- RJ45 Console Cable
- Rack Mount Kit
- Quick Installation Guide

*(all items must be in package to issue a refund):

Maximum data rates are based on IEEE 802.3ab standards. Actual throughput and range may vary depending on distance between devices or traffic and bandwidth load in the network. Features and specifications subject to change without notice. Trademarks and registered trademarks are the property of their respective owners. For United States of America: Copyright ©2014 EnGenius Technologies, Inc. All rights reserved. Compliant with FCC - This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his/her own expense.

Technical Specifications

Standard:

	EWS5912FP	EWS7928P	EWS7952FP
Ports	8	24	48
Power budget	Ports 1 - 8, output up to 30 Watts per Port	Ports 1 - 24, output up to 30 Watts per Port	Ports 1 - 48, output up to 30 Watts per Port
Total PoE Budget	130 W	185 W	740 W
SFP Slots	2	4	4
Switching Capacity:	24 Gbps	56 Gbps	104 Gbps
Forwarding Mode:	Store and Forward		
Flash Memory:	32 MB	32 MB	32 MB
SD RAM:	256 MB	256 MB	256 MB
MAC Address Table	8K		
Jumbo Frame	9K		

Port Functions:
8, 24, or 48 10/100/1000Mbps Ports in the front panel (Depending on model)
2 or 4 100/1000Mbps SFP Ports (Depending on model)
1 RJ 45 Port

PoE Capability:
PoE Standard: Port 1~8, 24, or 48 Support IEEE 802.3at/af
PoE Capable Ports:
Port 1~8, 24, or 48 can output up to 30 Watts

LED Indicator
Device:
Power LED x1
Fault LED x1
PoE Max LED x1
LAN Mode LED x1
PoE Mode LED x1
Copper Ports:
LAN/PoE Mode LED x 1
Link/Act LED x 1

SFP Ports:
Link/Act LED x 1

Environment & Mechanical:
Temperature Range
Operating: 32 to 122°F/0 to 50°C
Storage: -40 to 158°F/-40 to 70 °C
Humidity (non-condensing): 5% - 95%

L2 Features:

802.3ad compatible Link Aggregation
802.1D Spanning Tree (STP)
802.1w Rapid Spanning Tree (RSTP)
802.1s Multiple Spanning Tree (MSTP)
IGMP Snooping v1/v2/v3
MLD Snooping
IGMP Fast Leave
Port Trunking
Port Mirroring: One to one and many to one
VLAN Group
Voice VLAN
Queue
CoS based on 802.1p priority
CoS based on physical port
CoS based on TOS
CoS based on DSCP
BootP/DHCP Client
Firmware Burn-Proof
802.1X Port-based Access Control
802.1X Guest VLAN
Port Security
Port Isolation
Storm Control
Attack Prevention
Access Control List (ACL)
Telnet Server
TFTP Client
Web-based support
SNMP v1 support

L2 Features Continued:

SNMP v2c support
SNMP v3 support
TFTP upgrade
Command Line Interface (CLI)
SNTP
RMONv1
SYSLOG
Cable Diagnostics
MIB Support
RFC1213
RFC1493
RFC1757
RFC2674

PoE Management:

Power on/off per port
Power Class Configuration
Power feeding with priority
User-defined power limit

Wireless Management Features:

Wireless Network Management
Manage up to 20(EWS5912FP) / 50(EWS7928P, EWS7952FP) Access Points
- AP Auto Discovery and Provisioning
- AP Auto IP-Assignment
- AP Cluster Management

Wireless Configuration
- Remote AP Rebooting
- AP Device Name Editing
- AP Radio Settings
- Band Steering
- Traffic Shaping
- AP Client Limiting
- Fast Handover
- Fast Roaming
- Guest Network
- Wireless Security (WEP, WPA / WPA2 Enterprise, WPA-PSK / WPA2-PSK)
- VLANs for Access Point - Multiple SSID

Wireless Network Monitoring
- AP Status Monitoring
- Wireless Client Monitoring
- Wireless Traffic and Usage Statistics
- Visual Topology View
- Floor Plan View
- Map View

Wireless Network Security
- Secure Control Messaging
- SSL Certificate

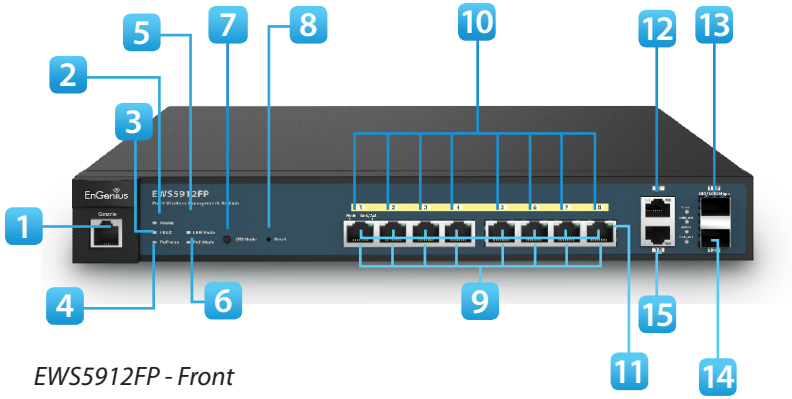
Management
- Local MAC Address Database
- Remote MAC Address Database (RADIUS)
- Unified Configuration Import/Export
- Intelligent Diagnostic
- Bulk Firmware Upgrade

Physical Interface

Dimensions

EWS5912FP

Width: 13” Length: 9” Height: 1.73”



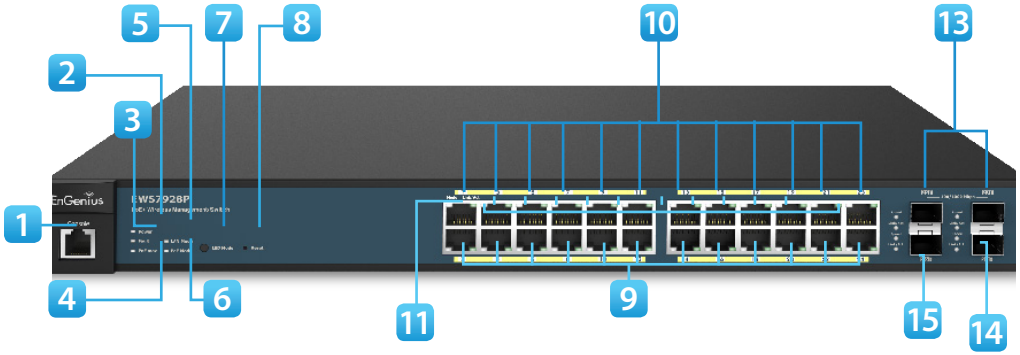
EWS5912FP - Front

EWS5912FP - Back

Dimensions and

EWS7928P

Width: 9.45” Length: 10.20” Height: 1.73”



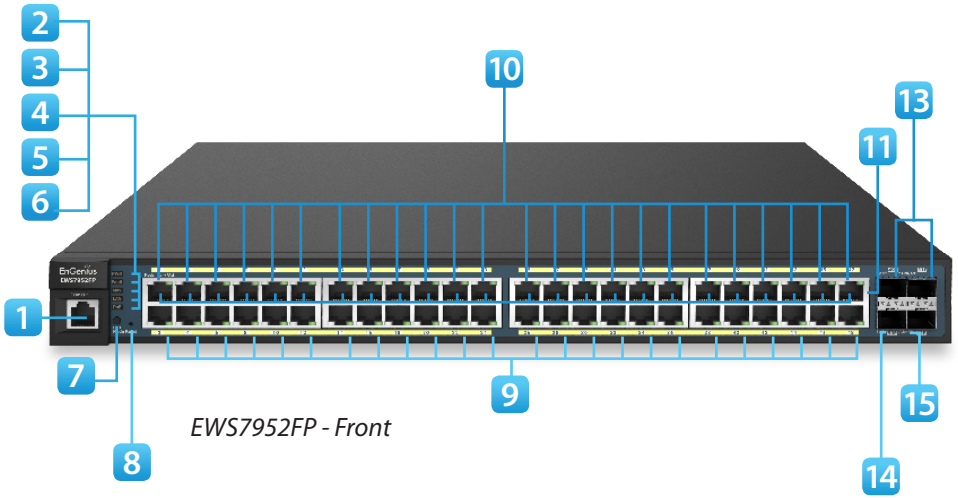
EWS7928P - Front

EWS7928P - Back

Dimensions

EWS7952FP

Width: 16.14” Length: 17.32” Height: 1.73”



EWS7952FP - Front

EWS7952FP -Back

1 **RJ45 Console Port**

2 **Power LED:** Light off = Power off; Solid Light = Power On.

3 **Fault LED:** Light off = Normal Behavior; Solid Light = Error.

4 **PoE Max LED:** Light off = Additional PoE device may still be added; Solid Light = The PoE device’s output power has exceeded total PoE limit. No additional devices can be powered on via PoE.

5 **LAN Mode LED:** Light off = LAN mode is not activated; Solid Light = LAN mode is activated.

6 **PoE Mode LED:** Light off = PoE mode is not activated; Solid Light = PoE mode is activated.

7 **LED Mode Selector:** Press to change between LAN and PoE mode.

8 **Reset Button:** Press to reset the device to factory default settings.

9 **RJ-45 LAN Ports:** 10/100/1000 Mbps RJ-45 LAN ports.

10 **LAN Mode LED (Per Copper Port):** Light off = No link is established on the port; Solid Amber Light = A valid 10/100 Mpbs link is established on the port; Solid Green Light = A valid 1000 Mbps link is established on the port.

11 **Link/Act LED (Per Copper Port):** Light off = No link is established on the port; Solid Light = A valid link is established on the port; Blinking Light = Packet transmission on the port.

12 **Uplink Ports:** Gigabit Ports

13 **SFP Ports:** Small form factor pluggable ports.

14 **Speed LED (Per SFP Port)**

15 **Link/Act LED (Per SFP Port):** Light off = No link is established on the port; Solid Amber Light: A valid 100 Mpbs link is established on the port; Solid Green Light: A valid 1000 Mbps link is established on the port.

16 **Power Connector**

Compatibility

Your EWS Wireless Management Switch supports the following Access Point models:

EnGenius EWS310AP Dual Band Wireless N600 Managed Indoor Access Point
EnGenius EWS320AP Dual Band Wireless N900 Managed Indoor Access Point
EnGenius EWS360AP Dual Band Wireless AC1750 Managed Indoor Access Point
EnGenius EWS610AP Dual Band Wireless N600 Managed Outdoor Access Point
EnGenius EWS620AP Dual Band Wireless N900 Managed Outdoor Access Point
EnGenius EWS660AP Dual Band Wireless AC1750 Managed Outdoor Access Point

*Future firmware releases will support additional models.

Management Interface

The Neutron Series EWS Layer 2 PoE+ Switch features an embedded Web interface for the monitoring and management of your device.

Connecting the Switch to a Network

Discovery in a Network with a DHCP Server

Use this procedure to setup the Switch within a network that uses DHCP.

1. Connect the supplied Power Cord to the Switch and plug the other end into an electrical outlet. Verify the power LED indicator is lit on the Switch.
2. Wait for the Switch to complete booting up. It might take a minute for the Switch to completly boot up.
3. Connect one end of a Category 5/6 Ethernet cable into the Gigabit (10/100/1000) Ethernet port on the Switch front panel and the other end to the Ethernet port on the computer. Verify that the LED on the Ethernet ports of the Switch are **green**.
4. Once your computer is on, ensure that your TCP/IP is set to **On** or **Enabled**. Open **Network Connections** and then click **Local Area Connecton**. Select **Internet Protocol Version 4 (TCP/IPv4)**. If your computer is already on a network, ensure that you have set it to a Static IP Address on the Interface (Example: 192.168.0.10 and the Subnet mask address as 255.255.255.0).
5. Open a web browser on your computer. In the address bar of the web browser, enter **192.168.0.239** and click **Enter**.
6. A login screen will appear. By default, the username is **admin** and the password is **password**. Enter the current password of the Switch and then click **Login**.
7. Once logged in, click **IP Settings** under the System tab and select IPv4 or IPv6.
8. Click **DHCP** under Auto-Configuration.
9. Click **Apply** to save the settings.
10. Connect the Switch to your network (DHCP enabled).
11. On the DHCP server, find and write down the IP address allocated to the device. Use this IP address to access the management interface.

Discovery on a Network without a DHCP Server

This section describes how to set up the Switch in a network without a DHCP server. If your network has no DHCP service, you must assign a static IP address to your Switch in order to log in to the web-based Switch management.

1. Connect the supplied Power Cord to the Switch and plug the other end into an electrical outlet. Verify the Power LED indicator is lit on the Switch.
2. Wait for the Switch to complete booting up. It might take a minute or so for the Switch to completely boot up.
3. Connect one end of a Category 5/6 Ethernet cable into the Gigabit (10/100/1000) Ethernet port on the Switch front panel and the other end to Ethernet port on the computer. Verify that the LED on Ethernet ports of the Switch are green.
4. Once your computer is on, ensure that your TCP/IP is set to **On** or **Enabled**. Open **Network Connections** and then click **Local Area Connecton**. Select **Internet Protocol Version 4 (TCP/IPv4)**.
5. If your computer is already on a network, ensure that you have set it to a Static IP Address on the Interface (Example: 192.168.0.10 and the Subnet mask address as 255.255.255.0).
6. Open a web browser on your computer. In the address bar of the web browser, enter **192.168.0.239** and click **Enter.**
7. A login screen will appear. By default, the username is **admin** and the password is **password**. Enter the current password of the Switch and then click **Login**.

   To make access to the web-based management interface more secure, it's highly reccomended that you change the password to something more unique.
8. Once logged in, click **IP Settings** under the **System** menu and select **Static IP** to configure the IP settings of the management interface.
9. Enter the IP address, Subnet mask, and Gateway.
10. Click **Apply** to update the system.

Use this procedure to access the management interface

Web Access

through a Web browser for device configuration.

1. Open a Web browser on your computer and enter the following address (default): **http://192.168.0.239**.

2. On the login screen, use the following information:
   Username: **admin**

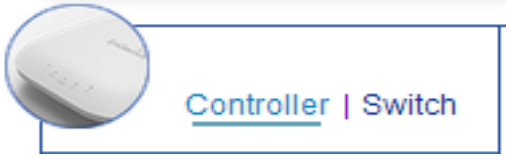
   Password: **password**

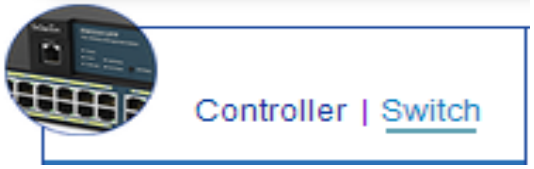
To make access to the web-based management interface more secure, it's highly reccomended that you change the password to something more unique.

Chapter 2
Controller Management

Wireless Controller & Layer 2 Switch

Besides having the Wireless Controller functions, the EWS Wireless Management Switch also possesses functions of a full-featured Layer 2 PoE switch. Use the Controller/ Switch tab on the upper left corner to toggle between the Wireless Controller or Layer 2 Switch functions.

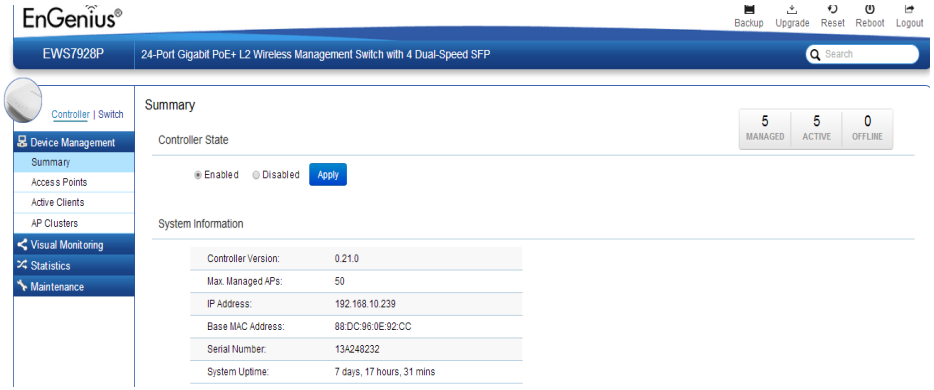




Device Management

Summary

The Summary page shows general system information for the EWS Switch including its software version, the maximum number of APs the EWS can manage, MAC Address, IP Address, serial number, and system uptime for the Switch. Select whether to **Enable** or **Disable** the Controller feature on the Switch. Next, click **Apply** to save the changes to the system.



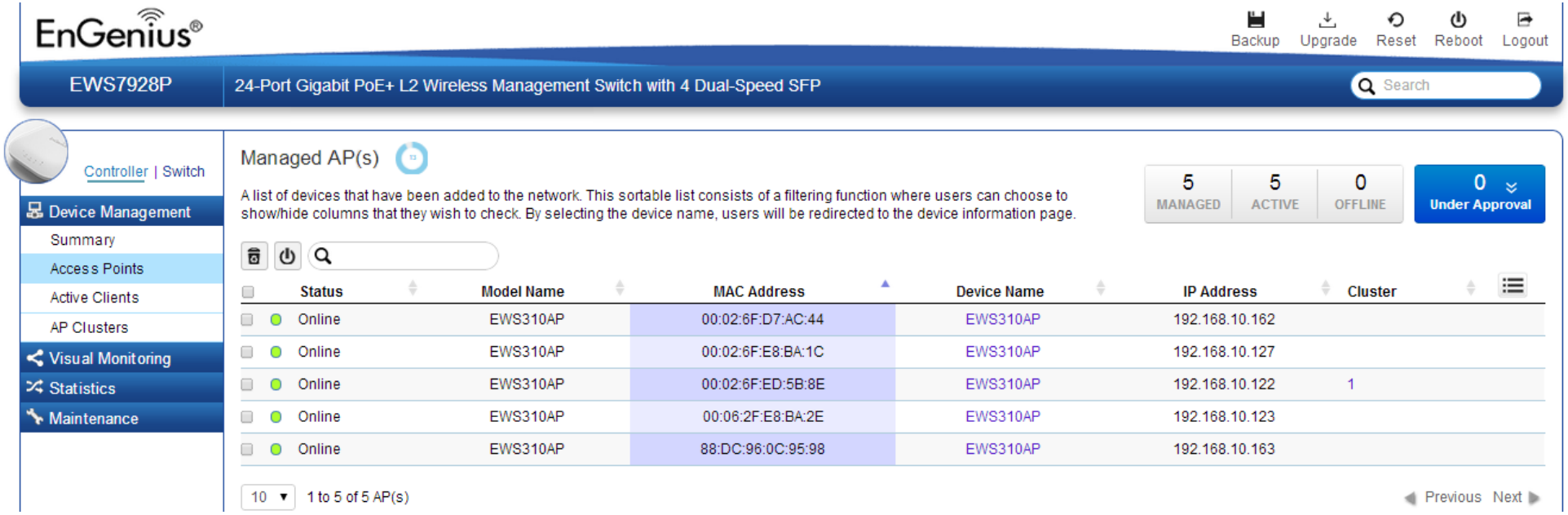
The Dashboard on the upper right corner of the GUI shows the current status of EWS AP(s) that has been managed by the EWS Switch.

Managed:	This shows the number of APs in the managed AP database that are configured with the EWS Switch.
Active:	This shows the number of managed APs that currently have an active connection with the EWS Switch.
Offline:	This shows the number of managed APs that currently do not have an active connection with the EWS Switch.
Controller State:	Click to enable or disable the EWS AP Controller feature.
Controller Version:	This is the software version of the device.
Max. Managed Access Points:	The maximum number of APs the device is able to manage.
IP Address:	The IP address of the device.
Base MAC Address:	Universally assigned network address.
Serial Number:	The serial number of the device.
System Uptime:	Displays the number of days, hours, and minutes since the last system restart.

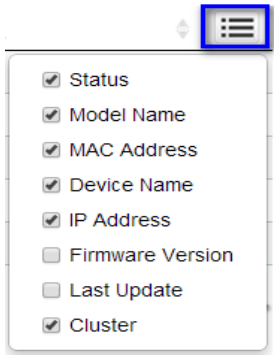
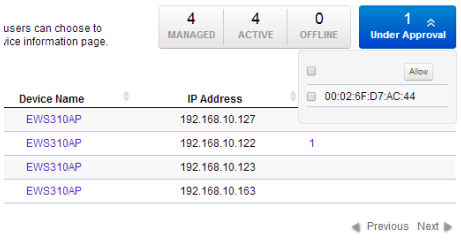
Access Points

This page displays the status of all EWS APs that your Controller is currently managing as well as all the EWS Access Points in the network that the Controller has discovered. Use this page to add EWS Access Points to your EWS Controller Access Point list. In the case of multiple Access Points, a filtering feature is enabled to help you to manage the Access Points connected by showing or hiding columns via the search bar or checking the corresponding box. Select a device and click on **Next** at the bottom right of the page to view details relating to the Access Point.

The EWS Wireless Management Switch is able to manage supported EnGenius Access Points. For the discovery procedure to succeed, the EWS Switch and the EWS Access point must be connected in the same network. The EWS Switch can discover supported EWS Access Points with any IP address and Subnet settings.

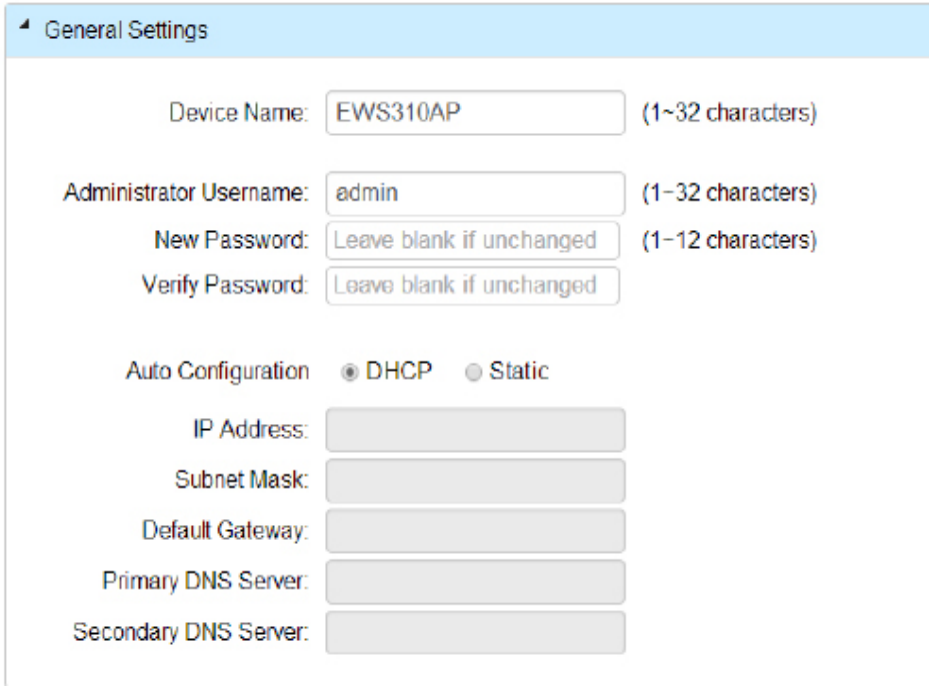


Refresh Countdown Timer:	This is the time left before the page auto-refreshes. The countdown is from 15 seconds.
Managed:	This is the number of Access Points in the managed Access Point database that are configured to the Controller.
Active:	This is the number of Access Points that currently have an active connection with the Controller.
Offline:	This is the number of Access Points that currently do not have an active connection with the Controller.
Managed APs:	This is a list of Access Points in the database that configured with the Controller.
Remove:	The Remove button romoves selected Access Points(s) from list. Access Points removed will be automatically set to standalone mode with all settings restored to their factory default settings.
Reboot:	The Reboot button will reboot the selected Access Point(s).
Search box:	Search for Access Points in the list using the following criteria: Status, model name, MAC Address, Device name, IP Address, Firmware Version, Cluster.
Status:	This indicates the current status of the managed Access Point.
Model Name:	Shows the model name of the managed Access Point.
MAC Address:	Shows the MAC address of the managed Access Point.

Device Name:	Displays the device name of the managed Access Point. Click on this field and you'll be redirected to the configuration page where you can edit settings such as device name, IP Address, Wireless Radio settings, SSID, etc.
IP Address:	Shows the IP Address of the managed Access Point.
Firmware Version:	Shows the firmware version of the managed Access Point.
Last Update:	Display the time the Access Point was last detected and the information was last updated.
Cluster:	Displays the Cluster the Access Point is currently assigned to. Click on this field and you'll be redirected to the cluster configuration page.
Column Filter: 	Shows or hides fields in the Access Point list.
AP Detected: 	Reveals a list of all APs in the network that the EWS Switch automatically discovers. Mouse over the discovered Access Point to show general information such as the MAC, IP, Model, FW, etc.
Add:	Select the Access Point you wish to have the Controller manage using the check box and click **ALLOW** to add to the Managed Access Point list.

General

From here you can view and configure general device information for selected Access Points that are connected to the network.



Global Settings

Select an Access Point to configure. Next, fill in the given information for the Access Point.

Device Name:	The device name of the Access Point. Users can enter a custom name for the Access Point if they wish.
Administrator Username:	Displays the current administrator login username for the Access Point. Enter a new Administrator username for the Access Point if you wish to change the username. The default username is: **admin.**
New Password:	Enter a new password of between 1~12 alphanumeric characters.
Verify Password:	Enter the password again for confirmation.

Auto Configuration

This section displays information about the selected Access Point. Select whether you wish to have **Static** or **DHCP** Auto-Configuration for the Access Point in relation to the Controller.

DHCP:	You can choose to auto assign IP Address if there is a DHCP server in the network.
Static:	If you wish to manually assign the IP Address, choose "Static". Enter the IP Address you wish to assign to the AP and fill in the subnet mask and default gateway (enter DNS server address if necessary)

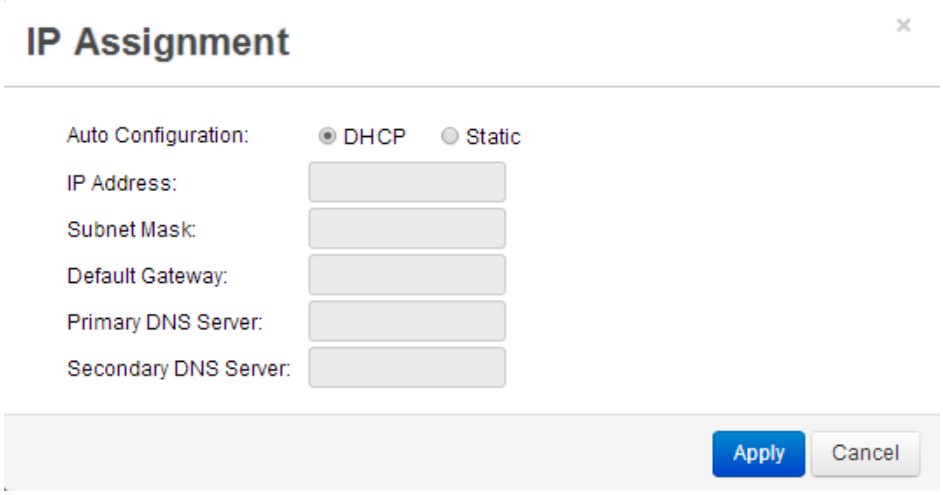
Auto-Configuration:	Select Static or DHCP for Auto-Configuration.
IP Address:	Enter the IP address for the Access Point.
Subnet Mask:	Enter the Subnet Mask for the Access Point.
Default Gateway:	Enter the default Gateway for the Access Point.
Primary DNS Server:	Enter the Primary DNS server name.
Secondary DNS Server:	Enter the secondary DNS server name.

How to Add Access Points to the Managed Access Point List

1. Access Points in the network will be automatically discovered by the EWS and will be listed in the **APs under Approval** list.

2. Select the Access Points(s) you wish to manage and click **Allow**.

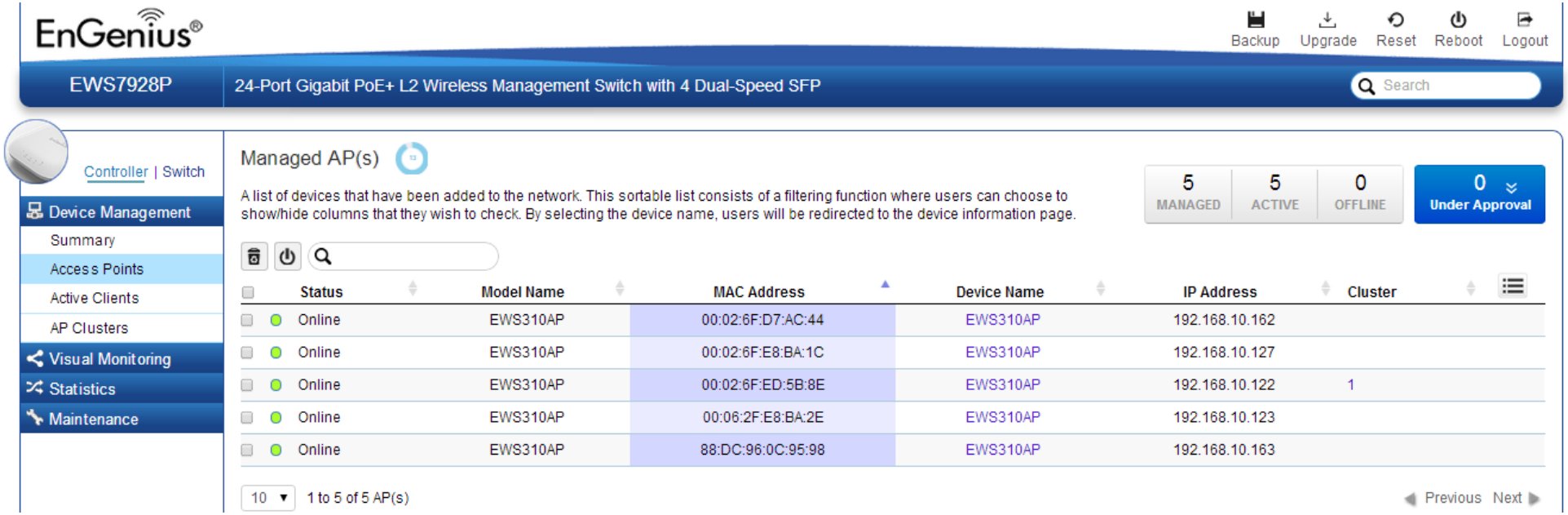
3. You will be prompted to assign the IP Address under the **IP Assignment** screen.



DHCP:	You can choose to auto assign an IP Address if there is a DHCP server in the network.
Static:	If you wish to manually assign the IP Address, choose "Static". Enter the IP Address you wish to assign to the AP(s) (if more than one AP is added, you'll be prompted to enter a range of IP Address) and fill in the subnet mask and default gateway (enter DNS server address if necessary).

4. Click **Apply** and the Access Points you've configured will be moved to the Managed list. Note that the status will change from **Connecting** to **Provisioning** to **Online**. Once you see **Online**, your Access Points(s) will have been successfully added to the Managed list.
Note that if the status is in the connecting mode for over 5 minutes, please check that the firmware of the Access Point and Switch match each other.

Individual Access Point Settings



Click on the **Device Name** field of the Access Point you wish to configure and you will be directed to a screen where you can configure settings for the Access Point.

Click **APPLY** to update the system settings.

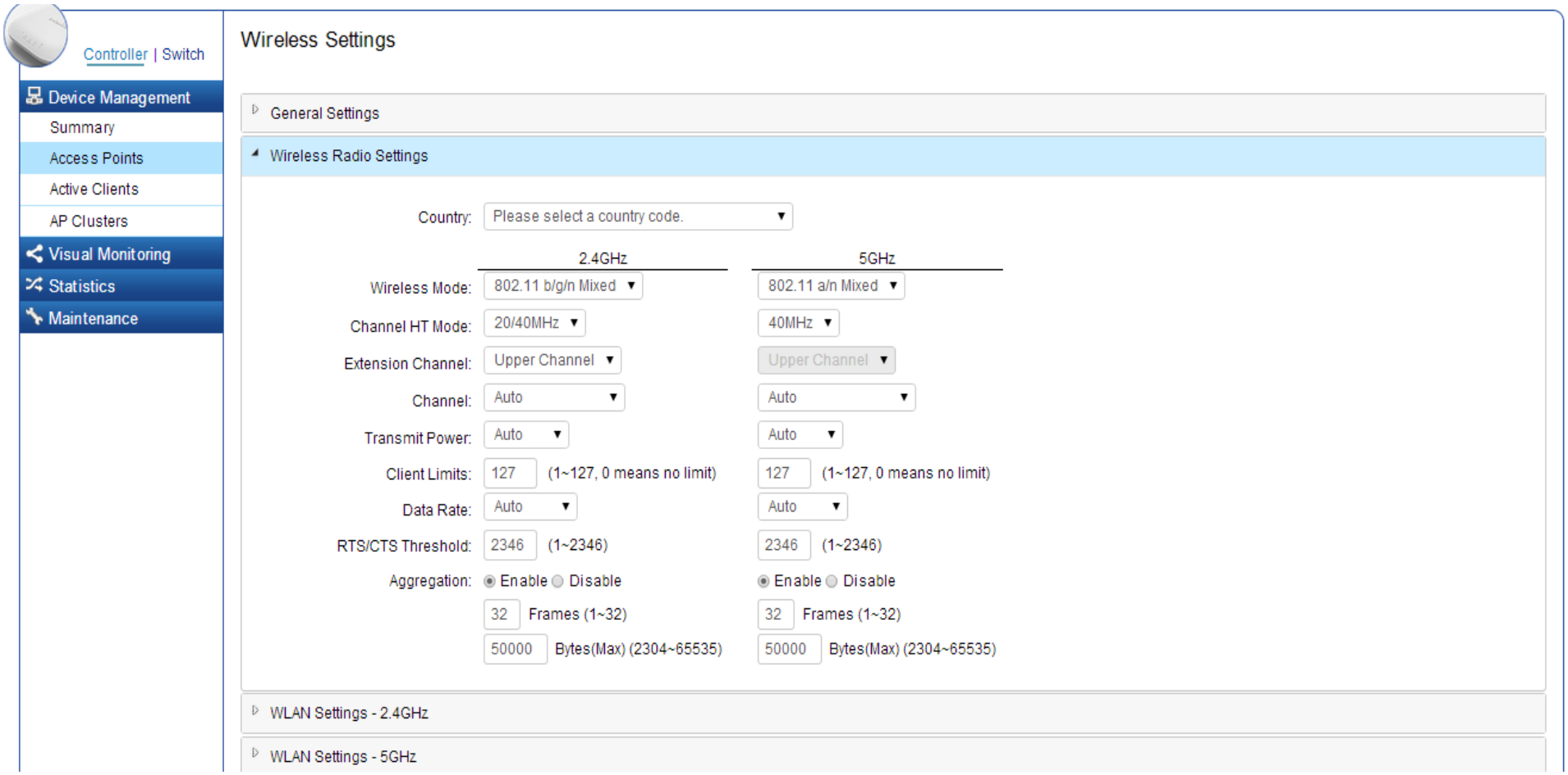
Wireless Radio Settings

2.4 GHz Settings

Under 2.4 GHz Settings, you can configure the radio settings of the selected Access Point.

5 GHz Settings

Under 5 GHz Settings, you can configure the radio settings of the selected Access Point.



Wireless Mode:	Select from the drop-down menu to set the wireless mode for the Access Point. For 2.4 GHz, the available options are 802.11b/g/n mixed, 802.11b, 802.11b/g mixed, 802.11g, and 802.11n. For 5 GHz, the available options are 802.11a/n mixed, 802.11a, and 802.11n.
Channel HT Mode:	Use the drop-down menu to select the Channel HT as 20 MHz, 20/40 MHz or 40 MHz. A wider channel improves the performance, but some legacy devices operate only on either 20MHz or 40 MHz. This option is only available for 802.11n modes.
Extension Channel:	Use the drop-down menu to select the Extension Channel as the **Upper** or **Lower** channel. An extension channel is a secondary channel used to bond with the primary channel to increase the range to 40MHz, allowing for greater bandwidth. This option is only available when Wireless Mode is 802.11n and Channel HT Mode is 20/40 MHz or 40 MHz.
Channel:	Use the drop-down menu to select the wireless channel the radio will operate on. Optimizing channel assignments reduces channel interference and channel utilization for the network, thereby improving overall network performance and increasing the network's client capacity. The list of available channels that can be assigned to radios is determined based on which country the Access Points are deployed in.

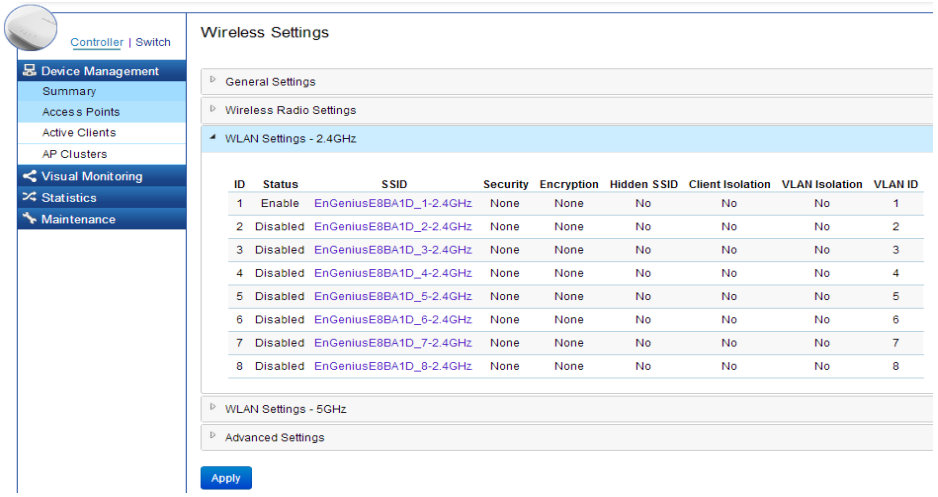
Transmit Power:	Use the drop-down menu to select the transmit power for the radio. Increasing the power improves performance, but if two or more Access Points are operating in the same area on the same channel, it may cause interference.
Client Limit:	Please specify the maximum number of wireless clients that can associate with the radio. Enter a range between 1~127, or fill in 0 for an unlimited client limit.
Data Rate:	Use the drop-down list to set the available data rates permitted for the wireless clients. The data rate will affect the throughput of the Access Point(s). The lower the data rate, the lower the throughput, but the longer the transmission distance.
RTS/CTS Threshold:	Enter a Request to Send (RTS) Threshold value between 1~2346. Use RTS/CTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same Access Point. Changing the RTS threshold can help control traffic flow through the Access Point. If you specify a lower threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce the throughput of the Access Point. Sending out more RTS packets can help the network recover from interference or collisions which might occur on a busy network or on a network experiencing electromagnetic interference.

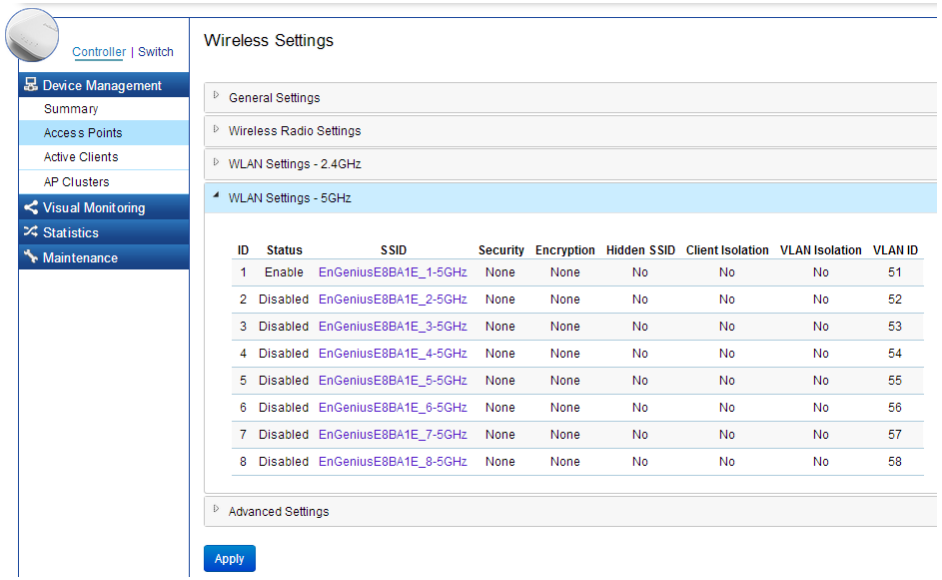
Aggregation:	Select whether to enable or disable Aggregation for the Access Point. This function merges data packets into one packet, reducing the number of packets. This also increases the packet sizes, so please keep this in mind. Aggregation is useful for increasing bandwidth throughput in environments that are prone to high error rates. This mode is only available for 802.11n modes. Fill in the frame rate limit you wish to use. The range is from 1~32. Next, fill in the max byte limit. The range is from 2304~65535.

Click **Apply** to save the changes to the system.

WLAN Settings - 2.4GHz/5GHz

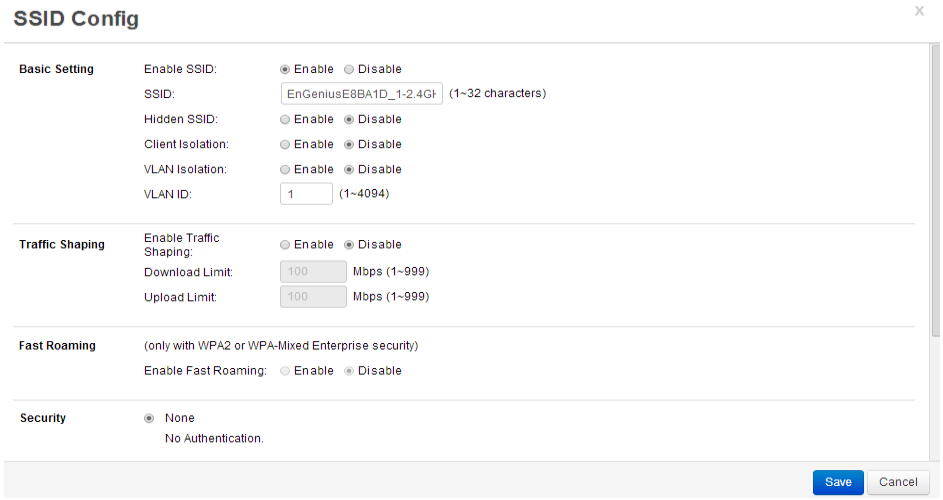
Under the WLAN Settings, you can create and manage SSID configurations and profiles for the Access Points to fit your needs. A SSID is basically the name of the wireless network to which a wireless client can connect to. Multiple SSIDs allow administrators to use a single physical network to support multiple applications with different configuration requirements. Up to 8 SSIDs are available per radio. Click on the SSID you wish to make changes to and you'll be directed to the SSID Configuration page.


Controller | Switch
Device Management
Summary
Access Points
Active Clients
AP Clusters
Visual Monitoring
Statistics
Maintenance
Wireless Settings
General Settings
Wireless Radio Settings
WLAN Settings - 2.4GHz
ID Status SSID Security Encryption Hidden SSID Client Isolation VLAN Isolation VLAN ID
1 Enable EnGeniusE8BA1D_1-2.4GHz None None No No No 1
2 Disabled EnGeniusE8BA1D_2-2.4GHz None None No No No 2
3 Disabled EnGeniusE8BA1D_3-2.4GHz None None No No No 3
4 Disabled EnGeniusE8BA1D_4-2.4GHz None None No No No 4
5 Disabled EnGeniusE8BA1D_5-2.4GHz None None No No No 5
6 Disabled EnGeniusE8BA1D_6-2.4GHz None None No No No 6
7 Disabled EnGeniusE8BA1D_7-2.4GHz None None No No No 7
8 Disabled EnGeniusE8BA1D_8-2.4GHz None None No No No 8
WLAN Settings - 5GHz
Advanced Settings
Apply


Controller | Switch
Device Management
Summary
Access Points
Active Clients
AP Clusters
Visual Monitoring
Statistics
Maintenance
Wireless Settings
General Settings
Wireless Radio Settings
WLAN Settings - 2.4GHz
WLAN Settings - 5GHz
ID Status SSID Security Encryption Hidden SSID Client Isolation VLAN Isolation VLAN ID
1 Enable EnGeniusE8BA1E_1-5GHz None None No No No 51
2 Disabled EnGeniusE8BA1E_2-5GHz None None No No No 52
3 Disabled EnGeniusE8BA1E_3-5GHz None None No No No 53
4 Disabled EnGeniusE8BA1E_4-5GHz None None No No No 54
5 Disabled EnGeniusE8BA1E_5-5GHz None None No No No 55
6 Disabled EnGeniusE8BA1E_6-5GHz None None No No No 56
7 Disabled EnGeniusE8BA1E_7-5GHz None None No No No 57
8 Disabled EnGeniusE8BA1E_8-5GHz None None No No No 58
Advanced Settings
Apply

ID:	The ID displays the SSID profile identifier.
Status:	This displays whether the current SSID profile is enabled or disabled.
SSID:	Displays the SSID name as it appears to the wireless clients in the network.
Security:	Displays the Security Mode the SSID uses.
Encryption:	Displays the Data Encryption type the SSID uses.
Hidden SSID:	Displays whether the hidden SSID is enabled or disabled.
Client Isolation:	Displays whether Client Isolation feature is enabled or disabled.
VLAN Isolation:	Displays whether VLAN Isolation feature is enabled or disabled.
VLAN ID:	Displays the VLAN ID associated with the SSID.

SSID Configuration



Basic Settings

Enable SSID:	Select to enable or disable the SSID broadcasting feature.
SSID:	Select the SSID for the current profile. This is the name that is visible to wireless clients on the network.
Hidden SSID:	Select **Enable** to hide the SSID from broadcasting. This can help to discourage wireless users from connecting to a particular SSID.
VLAN Isolation:	Select **Enable** to prevent wireless clients from communicating with any other device on a different VLAN.
VLAN ID:	Enter the VLAN ID for the SSID profile. The range is from 1~4094.

Traffic Shaping

Traffic Shaping regulates the flow of packets leaving an interface to deliver improved Quality of Service.

Enable Traffic Shaping:	Select to enable or disable Wireless Traffic Shaping for the Access Point.
Download Limit:	The Download Limit specifies the wireless transmission speed used for downloading. The range is from 1~999 Mbps.
Upload Limit:	The Upload Limit specifies the wireless transmission speed used for uploading. The range is from 1~999 Mbps.

Fast Roaming

When this function is enabled, PMKSA will be distributed and cached on neighboring Access Points to facilitate roaming. This function is only available with WPA2 or WPA-Mixed Enterprise security modes.

Enable Fast Roaming:	Select to enable or disable the Fast Roaming feature for the Access Point.

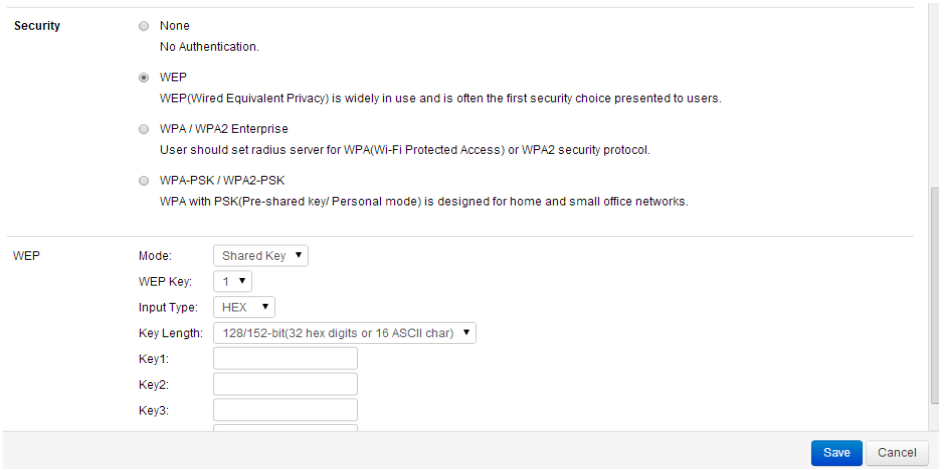
Security

The Security section allows users to select the security settings for the given wireless connection to protect the network. Select **None** to disable the Security feature for the network.

WEP

Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks which scrambles all data packets transmitted between the Access Point and the wireless clients associated with it. Both the Access Point and the wireless client must use the same WEP key for data encryption and decryption.

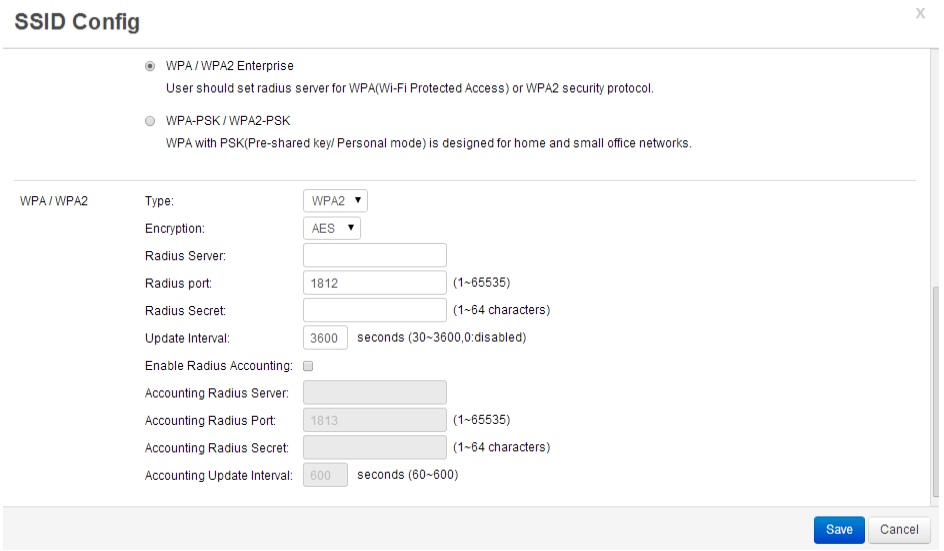
Mode:	Select **Open System** or **Shared Key**.
WEP Key:	Select the WEP Key you wish to use.
Input Type:	Select the key type. Your available options are ASCII and HEX. **ASCII Key:** You can choose upper and lower case alphanumeric characters and special symbols such as @ and #. **HEX Key:** You can choose to use digits from 0~9 and letters from A~F.
Key Length:	Select the bit-length of the encryption key to be used in the WEP connection. Your available options are: 64, 128, and 152-bit password lengths.
Key 1~4:	Based on your Key length selection, please enter the appropriate Key Value you wish to use.



WPA/WPA2 Enterprise

WPA and WPA2 are Wi-Fi Alliance IEEE 802.11i stadards, which include AES and TKIP mechanisms.

Type:	Select the WPA type to use. Available options are Mixed, WPA and WPA2.
Encryption:	Select the WPA encryption type you would like. Your available options are: Both, TKIP(Temporal Key Integrity Protocol) and AES(Advanced Encryption Standard).
Radius Server:	Enter the IP address of the Radius server.
Radius Port:	Enter the port number used for connections to the Radius server.
Radius Secret:	Enter the secret required to connect to the Radius server.
Update Interval:	Specify how often, in seconds, the group key changes. Select 0 to disable.
Radius Accounting:	Enables or disables the accounting feature.
Radius Accounting Server:	Enter the IP address of the Radius accounting server.
Radius Accounting Port:	Enter the port number used for connections to the Radius accounting server.
Radius Accounting Secret:	Enter the secret required to connect to the Radius accounting server.
Accounting Update Interval:	Specify how often, in seconds, the accounting data sends. The range is from 60~600 seconds.


SSID Config
WPA / WPA2 Enterprise
User should set radius server for WPA(Wi-Fi Protected Access) or WPA2 security protocol.
WPA-PSK / WPA2-PSK
WPA with PSK(Pre-shared key/ Personal mode) is designed for home and small office networks.
WPA / WPA2
Type: WPA2
Encryption: AES
Radius Server:
Radius port: 1812 (1~65535)
Radius Secret: (1~64 characters)
Update Interval: 3600 seconds (30~3600,0:disabled)
Enable Radius Accounting:
Accounting Radius Server:
Accounting Radius Port: 1813 (1~65535)
Accounting Radius Secret: (1~64 characters)
Accounting Update Interval: 600 seconds (60~600)
Save
Cancel

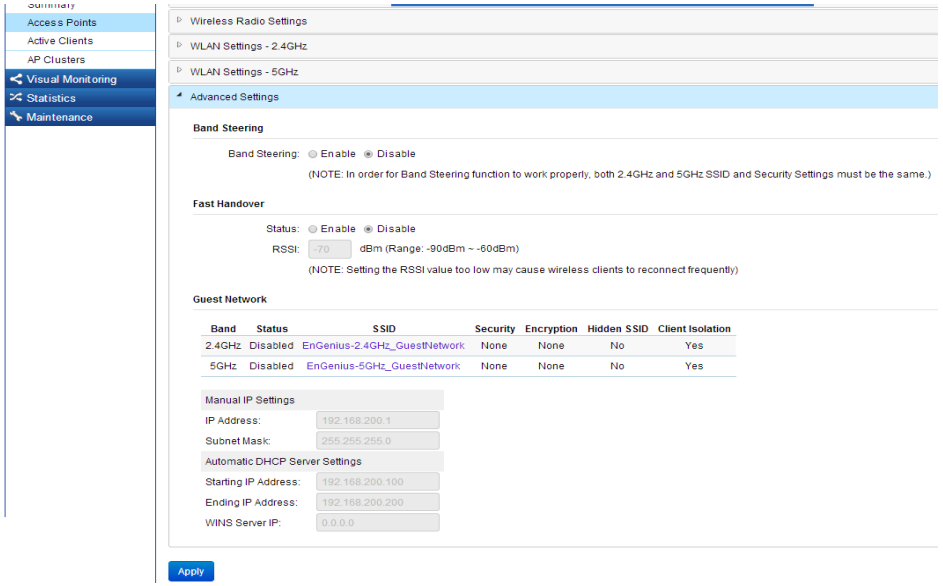
WPA-PSK/WPA2-PSK

WPA with PSK (Pre-shared key / Personal mode).

Type:	Select the WPA type you wish to use. Your available options are: Mixed, WPA-PSK, and WPA2-PSK.
Encryption:	Select the WPA encryption type you wish to use. Your available options are: Both or TKIP (Temporal Key)
PSK Key:	Select the PSK Key you wish to use. If using the ASCII format, the Key must be between 8~64 characters in length. If using HEX format, the Key must be 64 HEX characters in length.

Advanced Settings

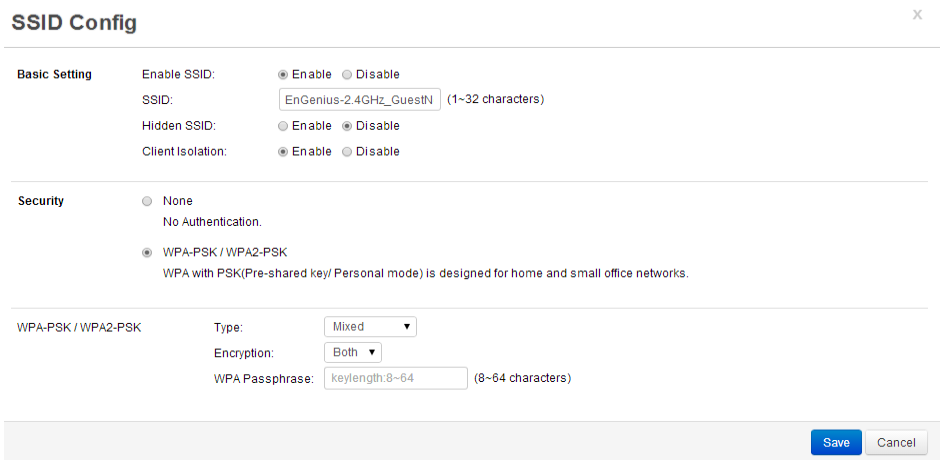
Click on the Advanced Settings tab to further customize your Access Point settings.


Access Points
Active Clients
AP Clusters
Visual Monitoring
Statistics
Maintenance
Wireless Radio Settings
WLAN Settings - 2.4GHz
WLAN Settings - 5GHz
Advanced Settings
Band Steering
Band Steering: Enable Disable
(NOTE: In order for Band Steering function to work properly, both 2.4GHz and 5GHz SSID and Security Settings must be the same.)
Fast Handover
Status: Enable Disable
RSSI: -70 dBm (Range: -90dBm ~ -60dBm)
(NOTE: Setting the RSSI value too low may cause wireless clients to reconnect frequently)
Guest Network
Band Status SSID Security Encryption Hidden SSID Client Isolation
2.4GHz Disabled EnGenius-2.4GHz_GuestNetwork None None No Yes
5GHz Disabled EnGenius-5GHz_GuestNetwork None None No Yes
Manual IP Settings
IP Address: 192.168.200.1
Subnet Mask: 255.255.255.0
Automatic DHCP Server Settings
Starting IP Address: 192.168.200.100
Ending IP Address: 192.168.200.200
WINS Server IP: 0.0.0.0
Apply

Band Steering	Click to enable or disable the Band Steering function for the Access Point. Note that the 2.4 GHz and 5 GHz SSIDs must have the same security settings.
Fast Handover:	With Fast Handover enabled, the Access Point will send a disassociation request to the wireless client and let it find another AP to handover and associate upon detecting the wireless client's RSSI value lower than specified. The RSSI value can be adjusted to allow for more clients to stay associated to this Access Point. Note that setting the RSSI value too low may cause wireless clients to reconnect frequently. The range is from -90 dBm~60 dBm.
Guest Network:	The Guest Network feature allows administrators to grant Internet connectivity to visitors or guests while keeping other networked devices and sensitive personal or company information private and secure.
Band:	Displays the radio band.
Status:	Displays whether the current SSID profile is enabled or disabled.
SSID:	Displays the SSID name as it appears to other wireless clients.
Security:	Displays the security Mode the SSID uses.
Encryption:	Displays the type of data encryption the SSID uses.
Hidden SSID:	Displays whether the hidden SSID is enabled or disabled.
Client Isolation:	Displays whether the Client Isolation feature is enabled or disabled.

Guest Network Configuration

Enable SSID:	Select to enable or disable SSID broadcasting on the network.
SSID:	Specify the SSID for the current profile. This is the name visible on the network to wireless clients.
Hidden SSID:	Select **Enable** to hide the SSID from broadcasting in order to discourage unauthorized wireless users from connecting to a particular SSID.
Client Isolation:	Select **Enable** to prevent wireless clients associated with an Access Point from communicating with other wireless devices.

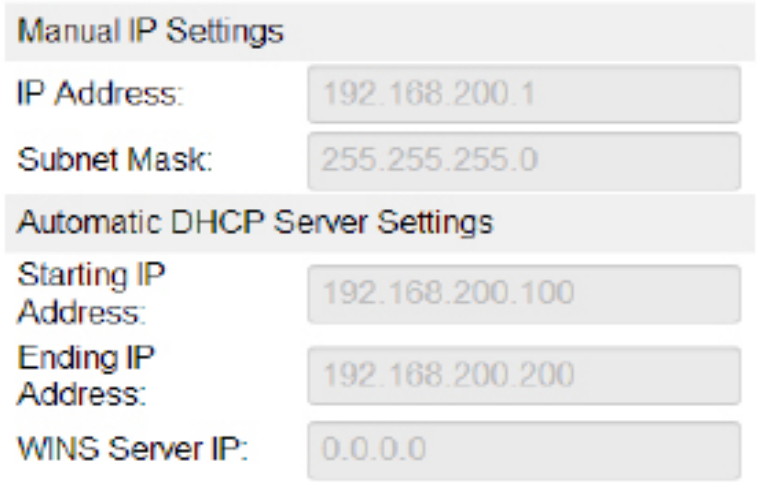


Security

None:	Select to disable security for the Access Point.
WPA-PSK/ WPA2-PSK	Select to enable WPA with PSK(Pre-shared key/ Personal mode) for the network. **Type**: Select the WPA type you wish to use. Your available options are: Mixed, WPA-PSK, and WPA2-PSK. **Encryption**: Select the WPA encryption type you wish to use. Your options are: Both or TKIP (Temporal Key) **PSK Key**: Specify the PSK Key you wish to use. If using ASCII format, the Key must be 8~64 characters. If using HEX format, the Key must be 64 HEX characters in length.

Manual IP Settings & Automatic DHCP Server Settings

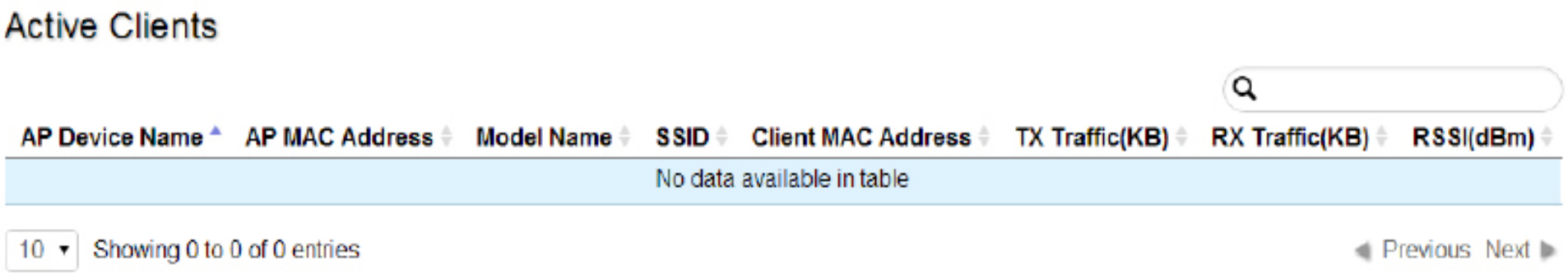
After enabling the Guest Network feature in the SSID Configuration page, enter IP address and Subnet mask for the Guest Network and assign an IP address range for wireless clients connecting to the Guest Network.



IP address:	Specify an IP address for the Guest Network.
Subnet mask:	Specify the Subnet mask IP address for the Guest Network.
Starting IP address:	Specify the starting IP address range for the Guest Network.
Ending IP address:	Specify the ending IP address range for the Guest Network.
WINS Server IP:	Specify the Windows Internet Name Service (WINS) Server IP address for the Guest Network. WINS is Microsoft's implementation of NetBIOS Name Service (NBNS), a name server and service for NetBIOS computer names.

Active Clients

From here, you can view information on the wireless clients that are associated with the Access Points that the EWS Switch manages. Click **Next** or **Previous** to view more parameters. If multiple Access Points are connected to the network, use the search bar to find an Access Point by its name.



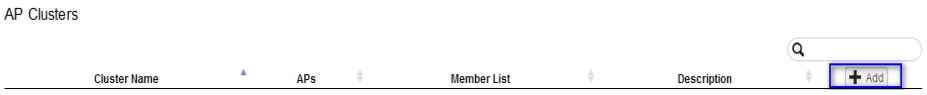
AP Device Name:	Displays the name of the Access Point which the client is connected to.
AP MAC address:	Displays the MAC address for the given Access Point.
Model Name:	Displays the model name for the Access Point.
SSID:	Displays the network on which the client is connected to.
Client MAC Address:	Displays the MAC Address of the Wireless Client connected to the Access Point.
TX Traffic(KB):	Displays the total traffic transmitted to the Wireless Client.
RX Traffics(KB):	Displays the total traffic received from the Wireless Client.
RRSS(dBm):	Displays the received signal strength indicator in terms of dBm.

AP Clusters

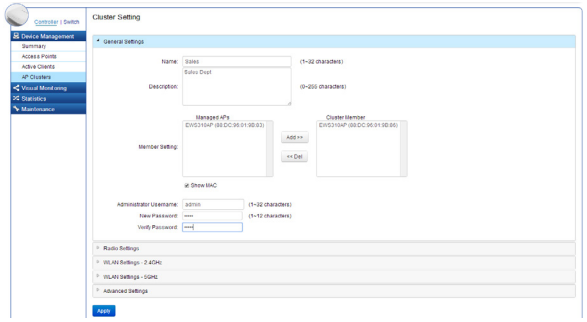
An Access Point Cluster is a dynamic, configuration-aware group of Access Points in the same subnet of a network. A cluster provides a single Access Point to manage the group of Access Points as a single wireless network instead of a series of separate devices. Clicking on the **Device Name** field of an Access Point that is already assigned to a cluster will direct you to a **Wireless Settings** page where you can only change the Device Name, Password & IP Settings of the Access Point selected. Wireless Radio settings can be configured for individual Access Points by overriding the cluster settings.

Cluster Name:	Displays the name of cluster group.
APs:	Displays the number of Access Points assigned to this cluster group.
Member List:	Displays the device name and MAC address of all Access Points assigned to this cluster group.
Description:	Show a description of the cluster group.

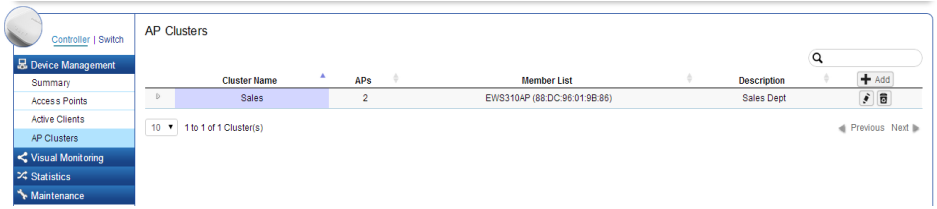
To manage a cluster on an Access Point:



Add: Creates a new Cluster



Edit: Edits Cluster settings for a cluster



Delete: Deletes a Cluster

1. Enter the name and description of the new cluster and choose your country from the drop-down menu.

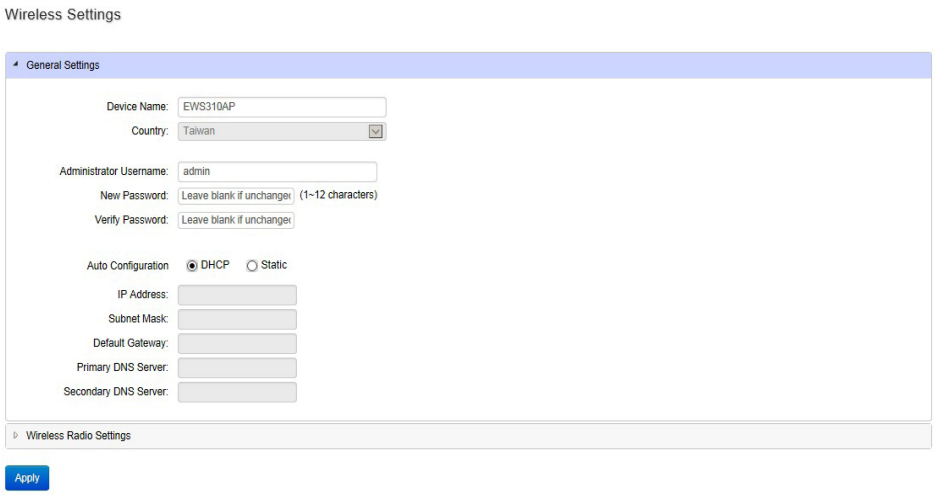
2. In the Member Setting section, all Access Points that are managed by the EWS Switch that are not currently assigned to a cluster will be listed on the left.

3. Select the Access Points you wish to assign to this cluster and press **Add**. The Access Points will be moved to the right column.

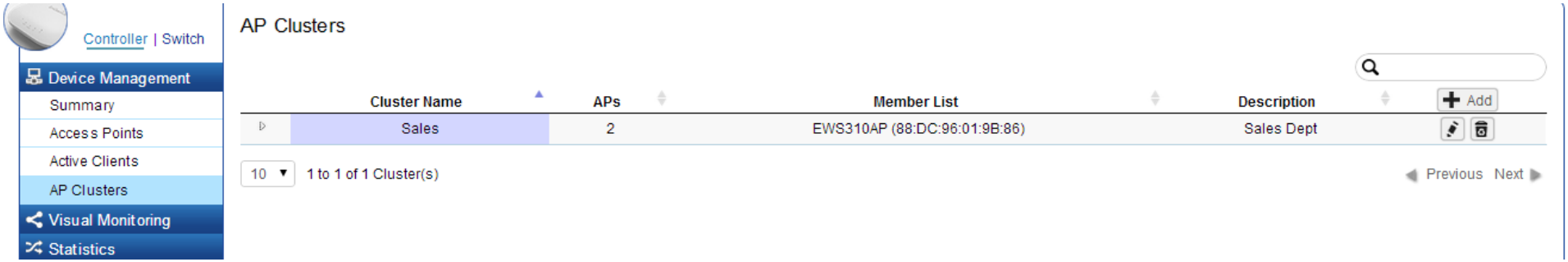
4. Configure Radio, WLAN, and Advanced settings then click on **Apply** for settings to take effect.

General

The General tab displays basic information about the Access Point cluster you are managing.



Name:	Enter the name of the cluster.
Country:	Select the location of the cluster from the drop-down box.
Description:	Enter a brief description about the cluster such as its purpose or importance.
Member Setting:	The Managed APs field will list all APs managed by the EWS Switch that are currently not currently assigned to another cluster. Click Add to assign it to this cluster or click Del to remove from this cluster.
Administrator Username:	The administrator login username for all the APs in this Cluster group. Enter a new Administrator Username if you want to change the default username. (Default value is admin)
New Password:	Enter a new password of between 1 and 12 alphanumeric characters.
Verify Password:	Enter password again for confirmation.



Member Settings

Click **Add** or **Delete** to manage the number of Access Points in the cluster.

Managed APs:	Shows the Access Points connected to the Controller.
Cluster Member:	Displays the Access Points that are a part of the cluster
Show MAC:	Check the box to display MAC addresses in addition to the Access Point names.

Click **Apply** to save the changes to the system.

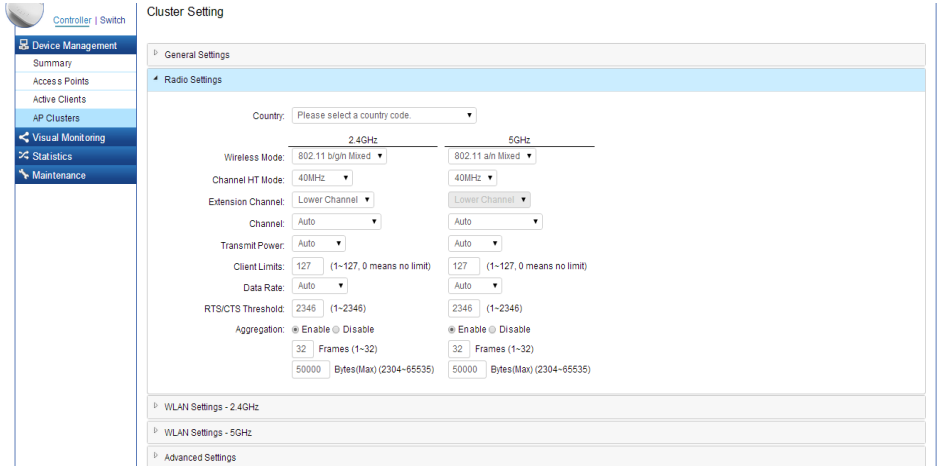
Autoconfiguration

DHCP:	You can choose to auto assign an IP address if there is a DHCP server in the network.
Static:	If you wish to manually assign the IP Address, choose "Static". Enter the IP Address you wish to assign to the AP and fill in the subnet mask and default gateway (enter DNS server address if necessary)

Radio Settings

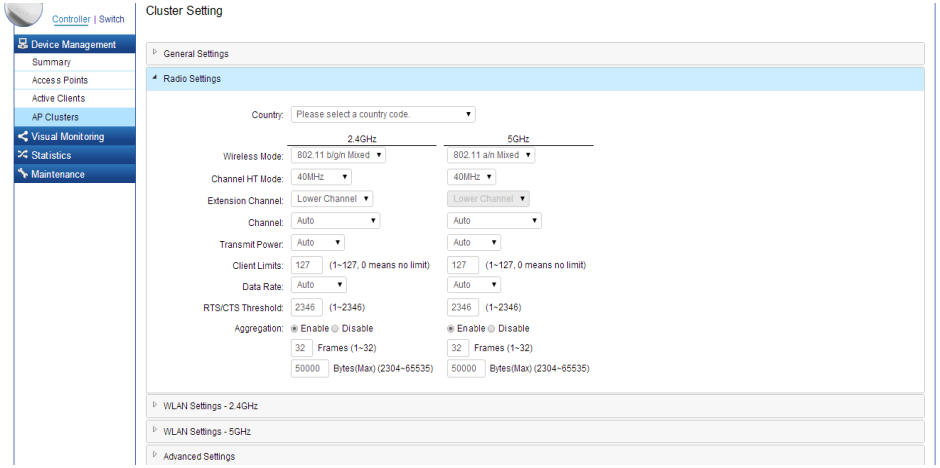
2.4 GHz/ 5 GHz Settings

From here, you can configure details about the cluster under the 2.4 GHz or 5 GHz band. Select and enter information regarding the types of channels for the cluster.



Country:	Enter the country that the Access Point resides in.
Override Cluster Settings:	Check this selection box if you wish to configure Wireless Radio Settings individually for the select Access Point.
Wireless Mode:	Use the drop-down menu to set the wireless mode for the access point. For 2.4GHz, available options are 802.11b/g/n mixed, 802.11b, 802.11b/g mixed, 802.11g, 802.11n only. For 5GHz, available options are 802.11a/n mixed, 802.11a, 802.11n only.
Channel HT Mode:	Use the drop-down menu to set the Channel HT as 20MHz, 20/40MHz or 40MHz. A wider channel improves the performance, but some legacy devices can operate only on either 20MHz or 40 MHz. This option is only available for 802.11n modes only.
Extension Channel:	Use the drop-down menu to set the Extension Channel as Upper or Lower channel. An extension channel is a secondary channel used to bond with the primary channel to increase this range to 40MHz allowing for greater bandwidth. This option is only available when Wireless Mode is 802.11n and Channel HT Mode is 20/40 MHz or 40MHz.
Channel:	Use the drop-down menu to set the wireless channel the radio will operate on. Optimizing channel assignments reduces channel interference and channel utilization, thereby improving overall network performance and increasing the network's client capacity. The list of available channels that can be assigned to radios is populated based on which country the APs are deployed in.

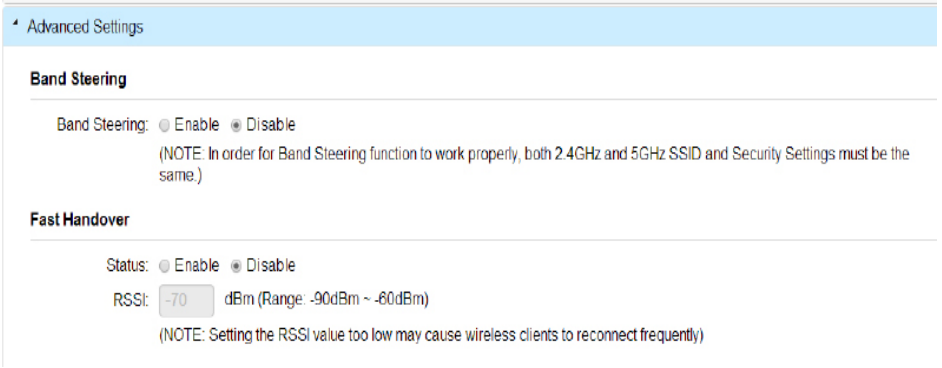
Transmit Power:	Use the drop-down menu to select the transmit power for the radio. Increasing the power improves performance, but if two or more access points are operating in the same area on the same channel, it may cause interference.
Client Limits:	Specify the maximum number of wireless clients that can associate with the radio. Enter a range between 1~127, or fill in 0 for an unlimited client limit.
Data Rate:	Enter the data rate you would like to use.
RTS/CTS Threshold:	Enter the RTS/CTS Threshold. The range is from 1~2346.
Aggregation:	Click to enable or disable the aggregation feature.
Frames:	Enter the amount of frames you wish to utilize. The range is from 1~32.
Bytes:	Enter the maximum limit of bytes. Your range is from 2304~65535.



Advanced Settings

Clicking on the cluster field of an Access Point will direct you to a Wireless Settings page where you can configure settings for the selected cluster.

Band Steering	Click to enable or disable the Band Steering function for the cluster. Note that the 2.4 GHz and 5 GHz SSIDs must have the same security settings.
Fast Handover:	With Fast Handover enabled, the Access Point will send a disassociation request to the wireless client and let it find another Access Point to handover and associate upon detecting the wireless client's RSSI value lower than specified. The RSSI value can be adjusted to allow for more clients to stay associated to this Access Point. Note that setting the RSSI value too low may cause wireless clients to reconnect frequently. The range is from -90 dBm~60 dBm.
Guest Network:	The Guest Network feature allows administrators to grant Internet connectivity to visitors or guests while keeping other networked devices and sensitive personal or company information private and secure.


Advanced Settings
Band Steering
Band Steering: Enable Disable
(NOTE: In order for Band Steering function to work properly, both 2.4GHz and 5GHz SSID and Security Settings must be the same.)
Fast Handover
Status: Enable Disable
RSSI: -70 dBm (Range: -90dBm ~ -60dBm)
(NOTE: Setting the RSSI value too low may cause wireless clients to reconnect frequently)

Manual IP Settings

IP address:	Specify an IP address for the Guest Network.
Subnet mask:	Specify the Subnet mask IP address for the Guest Network.
Starting IP address:	Specify the starting IP address range for the Guest Network.
Ending IP address:	Specify the ending IP address range for the Guest Network.
WINS Server IP:	Specify the Windows Internet Name Service (WINS) Server IP address for the Guest Network. WINS is Microsoft's implementation of NetBIOS Name Service (NBNS), a name server and service for NetBIOS computer names.

Automatic DHCP Server Settings

Starting IP address:	Enter the staring IP adrress that you would like to use.
Ending IP address:	Enter the final IP address that you would like to use.
WINS Server IP:	Enter the WINS Server IP adress for the cluster.

Apply: Click **APPLY** to update the the system settings.

Visual Monitoring

Topology View

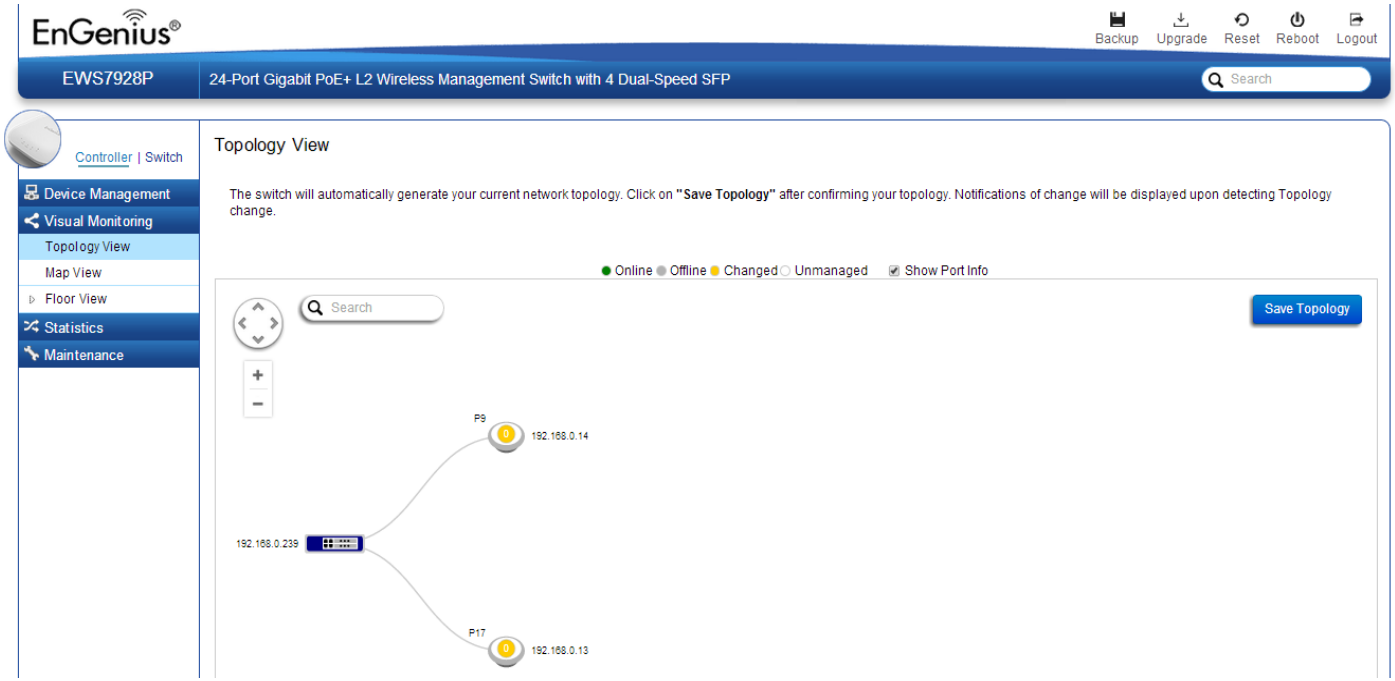
From here, you can see a visual view of the topology of the cluster in the netwrok. Use the directional pad and the plus or minus buttons to navigate your view of the network.

You can also search Access Points in the network via their IP or MAC address. Check the **Show Port Info** box to show whether you wish the search query to show port information.

The following table explains the color coding of Access Points in the topology view.

Green:	Online
Grey:	Offline
Yellow:	Status Change
White:	Unmanaged

Click the **Save Topology** button to update your settings.



Navigating Tips

Use to scroll up, down, left, or right.

Use to Zoom in/out. Alternatively, you can use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out.

Mouse over a device to show information about the device.

Left click on the Switch to redirect to the Switch UI on the collapsible topology tree.

Left click on the Access Point to redirect to the Active Clients page.

You can search for an Access Point using the IP Address or MAC address.

Click the **Show Port Info** box to show or hide port information on the Controller.

Click on

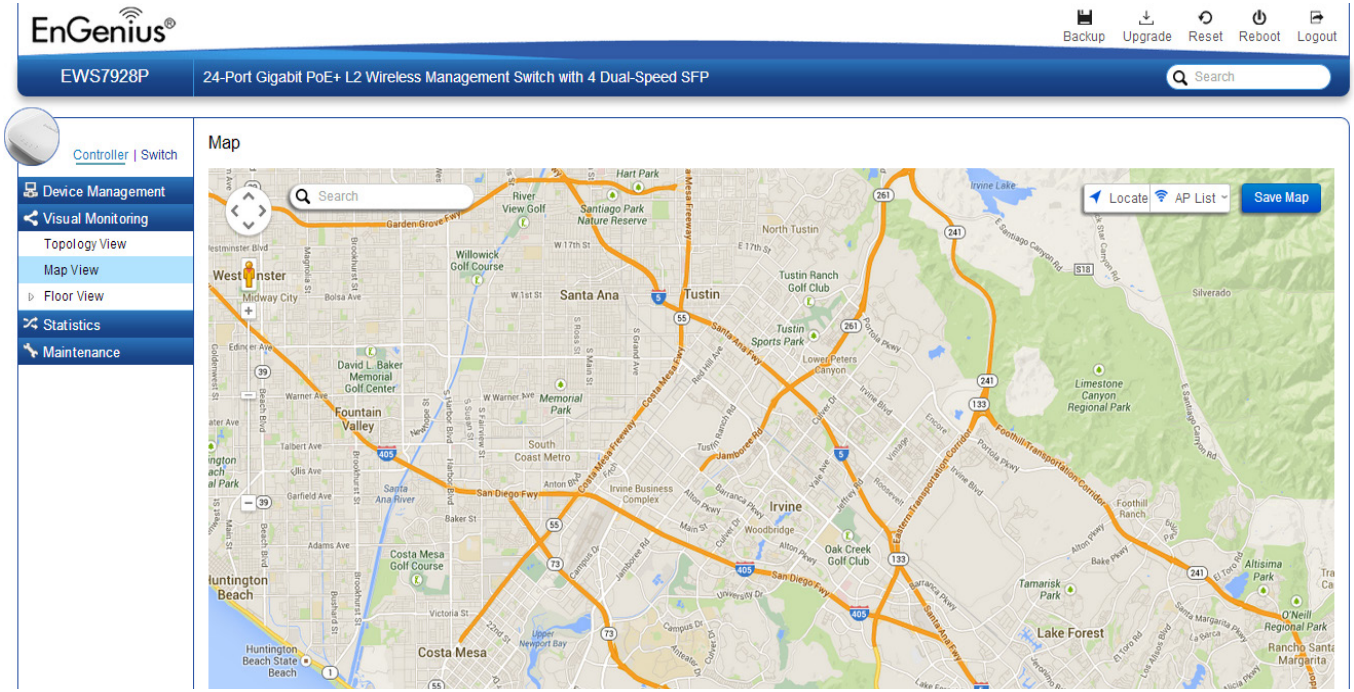
for the Controller to save the current network topology. Changes will be displayed upon detecting a topology change.

Map View

From here, you can view a realistic representation of Access Points in the network. To find Access Points within the network, enter the Access Point name in the search bar. Click **Hide AP List** to hide the Access Point list on the page or AP List to show a list of connected Access Points.

Status:	Displays whether the Access Point in the network is active or inactive.
Device Name:	Displays the name of the Access Point.

Click **Save Map** to save your preferences.

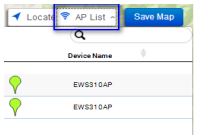


Navigating Tips

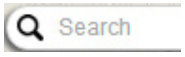
Use the directional pad to scroll up, down, left, or right.

Use the slider to zoom in/out. Alternatively, you can use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out.

Green:	Online
Grey:	Offline
Yellow:	Status Change
White:	New Device

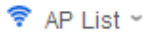


The number in the marker represents the number of wireless clients currently connected to the Access Point.



Use the Search box to search for locations by typing an address or the name of a landmark.

Use the Location button to pinpoint the map to your current location.



Click **AP List** to reveal a list of Access Points that the Controller is currently managing.

Click on **Save Map** for the settings to take effect.

To use the Map View:

1. Click on to display the list of managed Access Points.

2. Drag-and-drop the marker of the Access Point to the location on the map you wish to place.

3. Click on to complete.

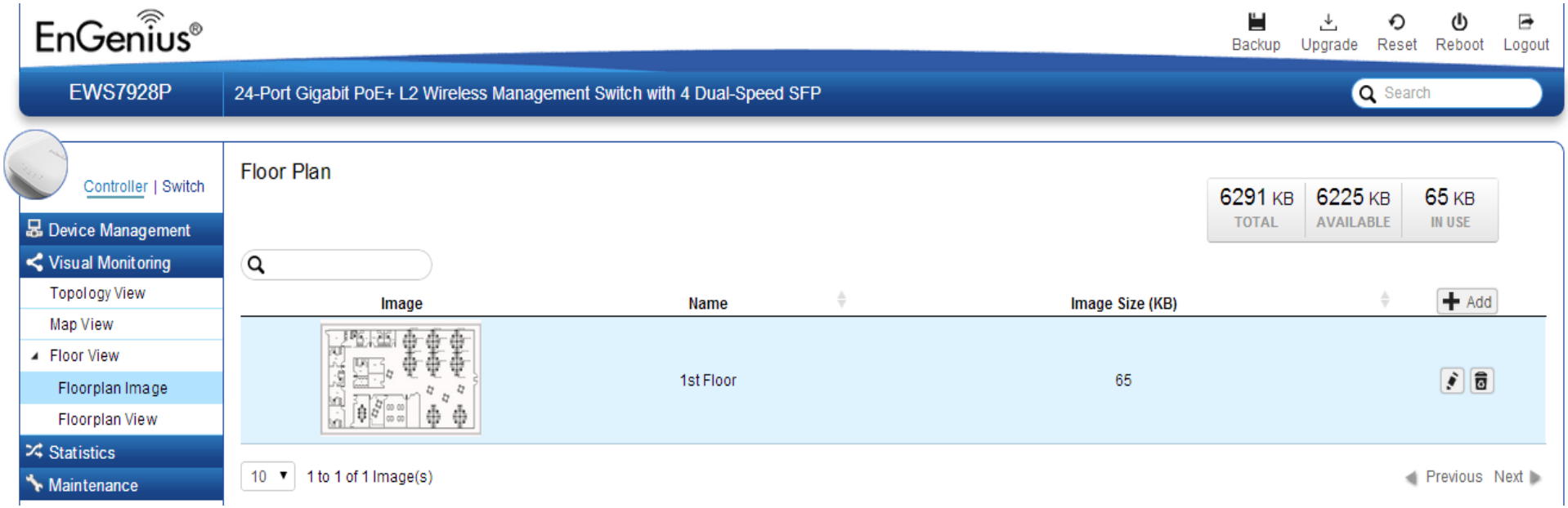
You can now easily locate you Access Point by mousing over the **Device Name** field in the Access Point List.

Floor View

The Floor View feature enables an administrator to upload custom floorplans for better network visualization of a wireless network. Multiple images can be uploaded to visualize Access Point placement on multiple floors of an office building or different branch offices within an organization.

Floorplan Image

From here, an administrator can add or delete a custom map or floorplan image.



Status Dashboard

Total:	Displays the total memory storage space allocated for uploading custom floorplans.
Available:	Display the memory storage space that is currently available.
In Use:	Displays the memory storage space that is currently in use.
Image:	Shows a preview of a custom uploaded image.
Name:	Shows the name of the custom uploaded image.
Image Size:	Displays th e file size of the custom uploaded image.

Managing Images

Add: Uploads a new image. The campatible formats are: GIF, PNG or JPG format, up to 819 KB per image.

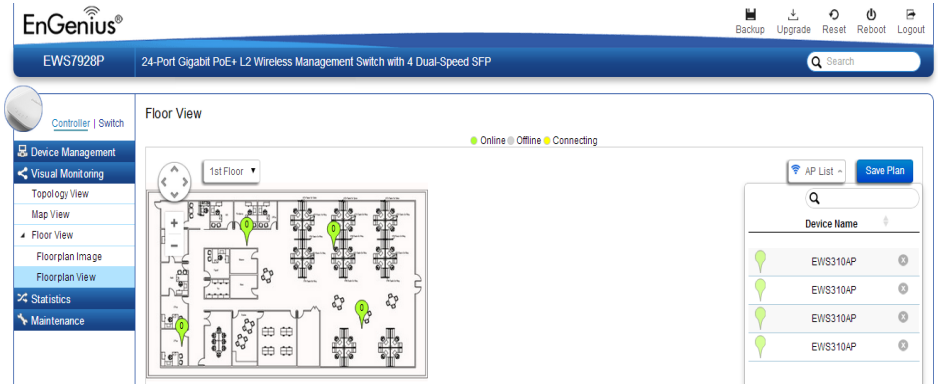
Edit: Edits the name of the uploaded image.

Delete: Removes an uploaded image.

Floorplan View

Floor View

From this page, the administrator can place Access Points onto the custom uploaded image by drag-ging-and-dropping markers in the Access Point list.



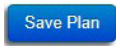
Navigating Tips

Use to scroll up, down, left, or right.

Use to Zoom in/out. Alternatively, you can use the mouse to navigate by clicking and dragging the left mouse button. Use the mouse wheel to zoom in/out.

The number in the marker represents the number of wireless clients that are currently connected to the Access Point.

AP List: Click to reveal a list of APs that the EWS Switch is currently managing.



Save Plan: Click for settings to take effect.

Color Legend

Green:	Online - There is an active connection with the EWS Switch.
Grey:	Offline - There is no active connection with the EWS Switch.
Yellow:	Status Change - Indicates that there has been a status change for the managed Access Point.
White:	New Device - An Access Point has been recently added to the network.

How to use the Floorplan View

1. Click on the **AP List** button to display the list of managed Access Points.

2. Drag-and-drop the green flag marker representing the Access Point to a location on the map.

3. Click on **Save Plan** to save your changes.

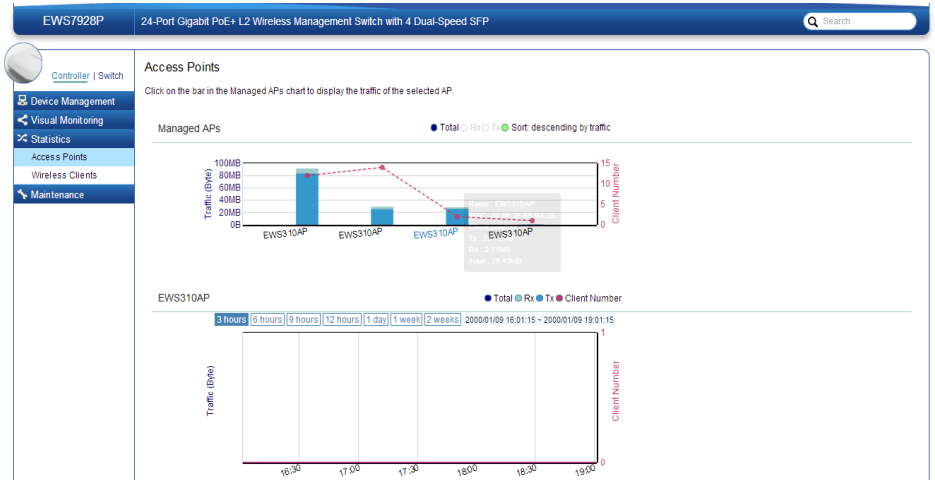
You can now easily locate you Access Point by having your mouse cursor over the **Device Name** field in the Access Point List.

Statistics

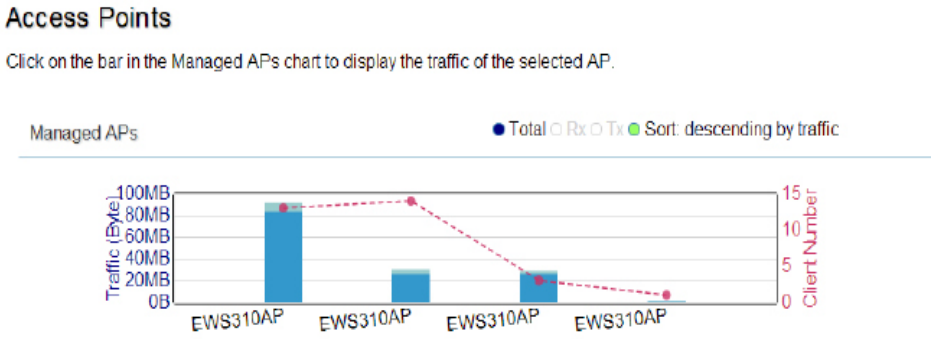
The Statistic page provides a convenient overview of Access Points and client traffic for the network.

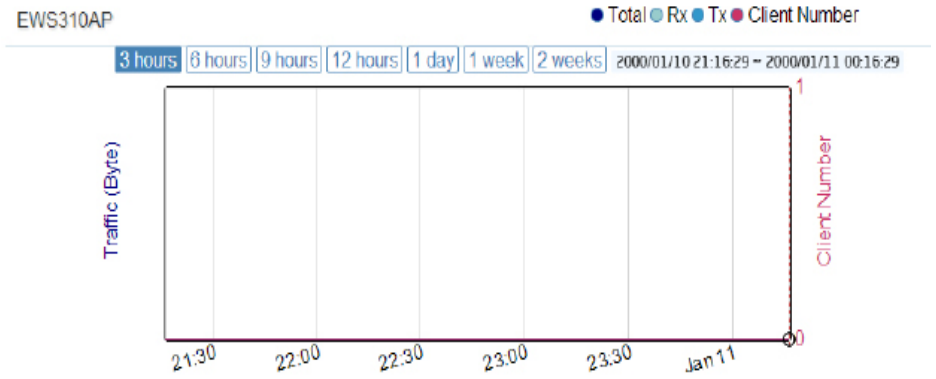
Access Points

The page displays a visual chart of the network traffic of all the Access Points managed by the EWS Switch. Click **Sort** to view your results for the collective usage of all Access Points on the Network.

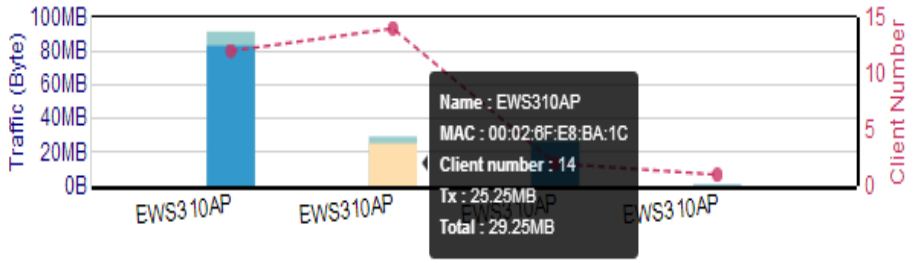


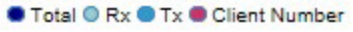
Total, Rx, Tx:	Use the buttons to toggle between Total Traffic, Rx Traffic, or Tx Traffic.
Sorting:	Use this button to sort the order from ascending/ descending, depending on your preference.



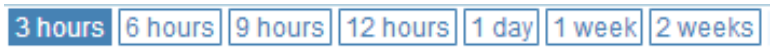


Place your mouse cursor over a bar in the chart to show details of the AP. Next, click on the bar to show the traffic of the Access Point in a chart.





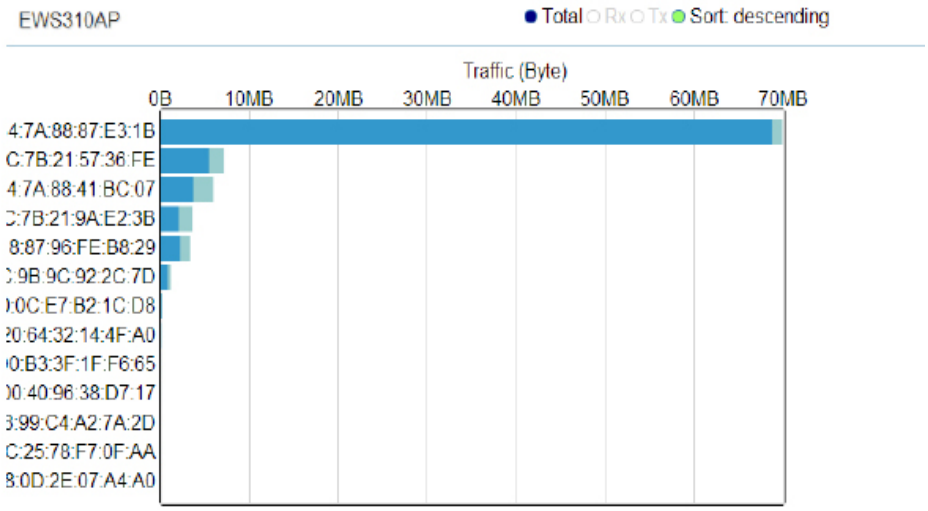
Total, Rx, Tx, Client Number: Use the button to toggle show/hide Total Traffic, Rx Traffic, Tx Traffic, Client Number.

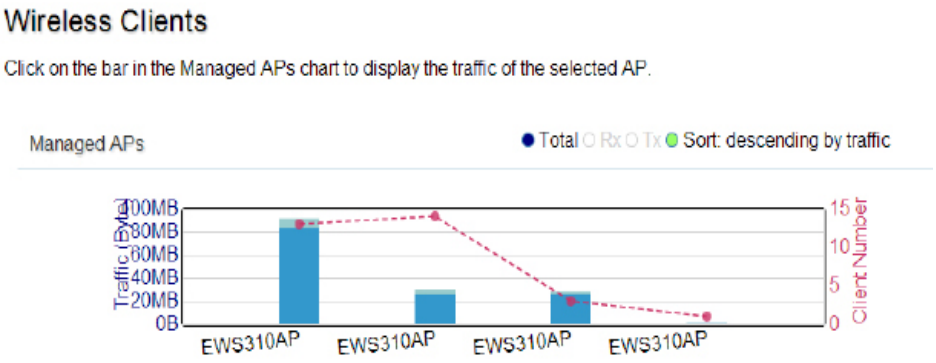


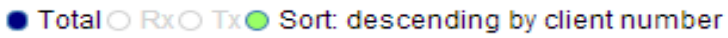
Select a time increment to monitor statistics by: 3 hrs, 6 hrs, 9 hrs, 12 hrs, 1 day, 1 week, or 2 weeks.

Wireless Clients

In addition to viewing information based on specific Access Points, you can view data via specific clients as well for secuirty purposes. Select the Access Point you wish to view and check whether you wish to include Tx, Rx, or total usage for the client. Next, click **Sort** to view your results.

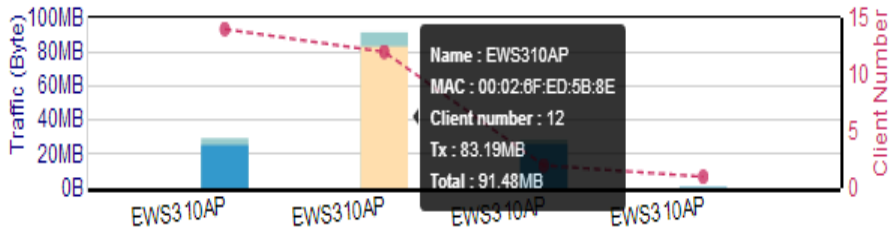




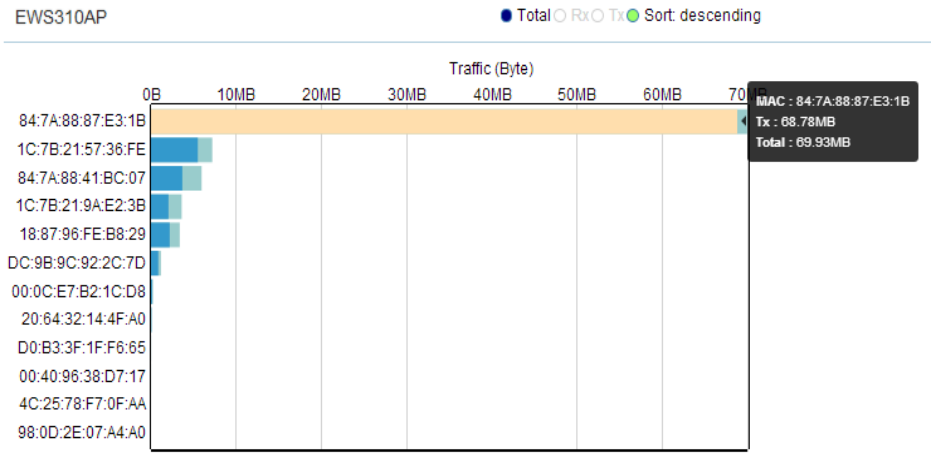


Total, Rx, Tx: Use the buttons to toggle between Total Traffic, Rx Traffic, and Tx Traffic.
Sorting: Use this button to sort the order to ascending/ descending.

Total, Rx, Tx: Use the buttons to toggle between Total Traffic, Rx Traffic, and Tx Traffic.
Sorting: Use this button to sort the order to ascending/ descending.



Place your mouse cursor over a bar in the chart or on the name of an Access point to show details of a selected Access Point. Next, click on the bar to show the traffic of the Access Point in a chart.



Place mouse cursor over a bar in the chart to show details of the wireless client.

Maintenance

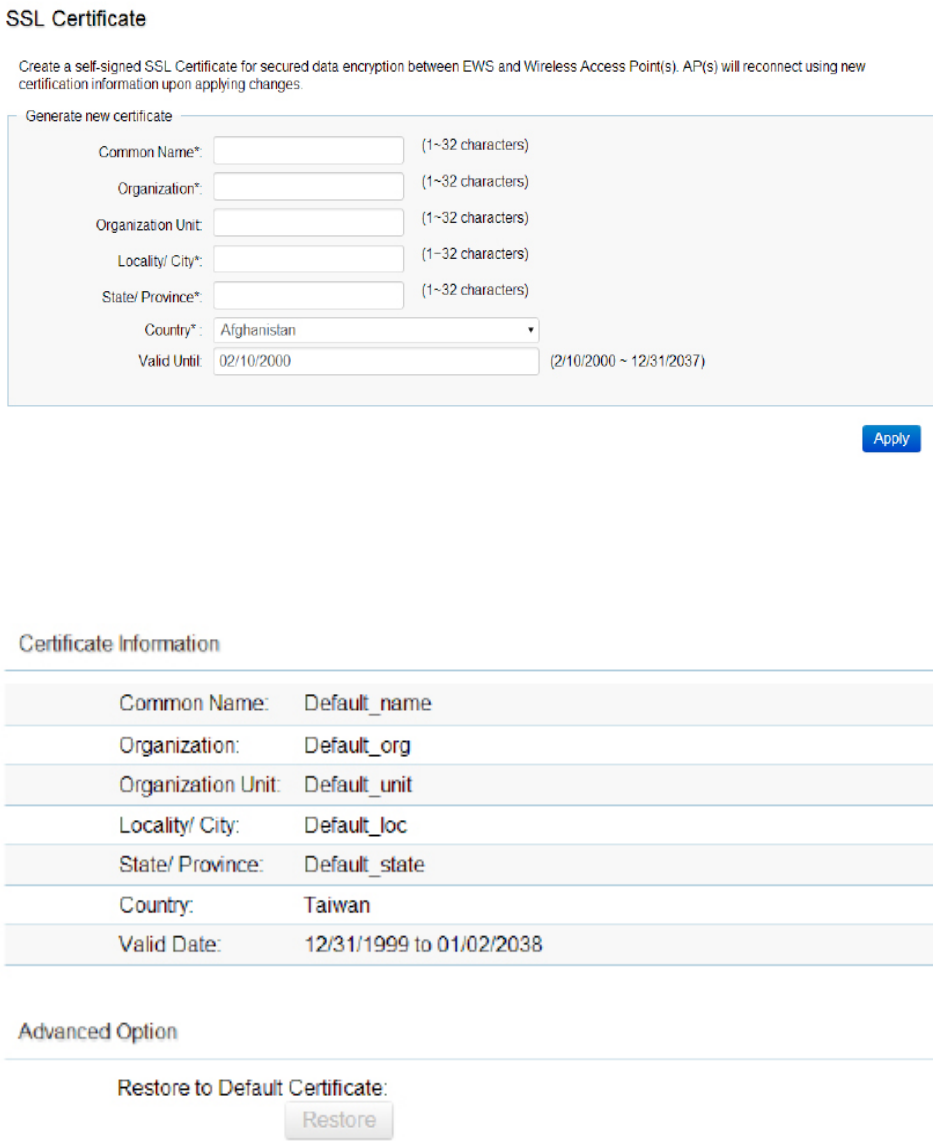
SSL Certificate

The Secure Socket Layer protocol is used to ensure secure transactions and transmissions between web servers and browsers. An SSL certificate serves as an electronic passport that establishes an online entity's credentials when accessing the Web. When a user attempts to send confidential information to a Web server, the user's browser must access the server's digital certificate and establishes a secure connection. Administrators can create a self-signed SSL Certificate to secure communications between the Switch and Access Points. Note that Access Points will disconnect and reconnect using new certificate upon applying changes.

Generate a New Certificate

Enter the information below to generate a request for an SSL certificate for the controller.

Common Name:	Enter the name of the request.
Organization:	Enter the organizations name.
Organization Unit:	Enter a unit name (department, etc.).
Locality/City:	Enter the locality or city.
State/Province:	Enter the state or province.



Apply: Click **APPLY** to update the the system settings.

Certificate Information

This area will display information about the given certificate. Click **Display Certificate Information** to show the current certificate information.

Advanced Options

This area will show any advanced options chosen.

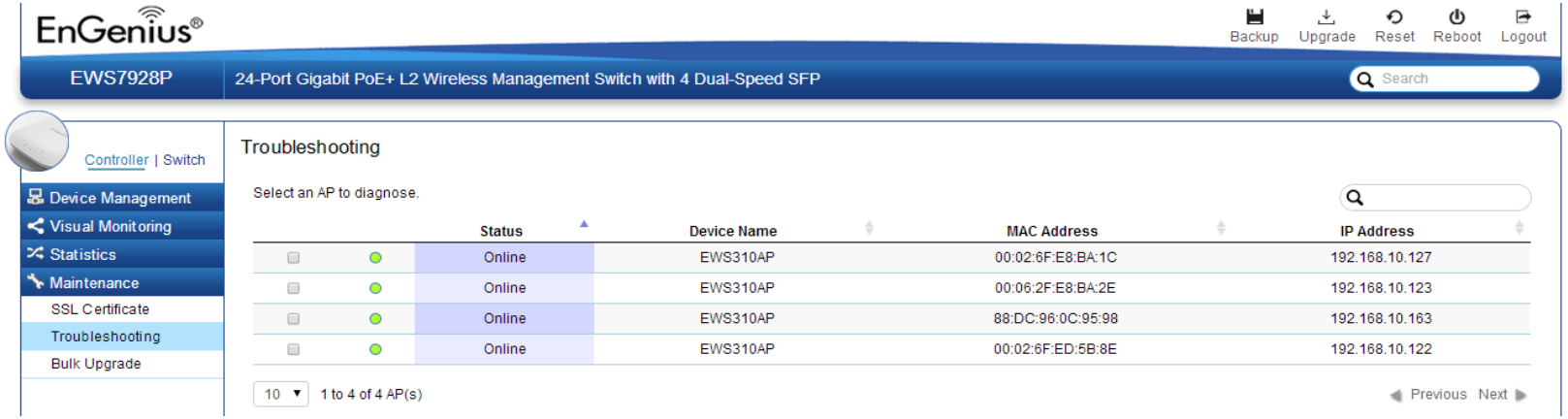
Click on **Restore** under Advance Options to restore the default SSL Certificate settings. Click **APPLY** to update the the system settings.

Trouble Shooting

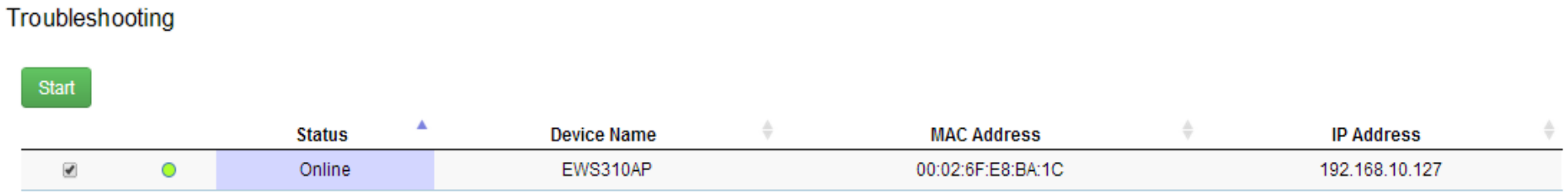
From here, you can troubleshoot any issues you have with Access Points connected to the network. This feature is designed primarily for administrators to verify and test the link route between the Switch and the Access Point. A troubleshooting solution is provided by the system so that administrators can know where the problem lies. Note that the topology of the network needs to be saved for this function to work properly.

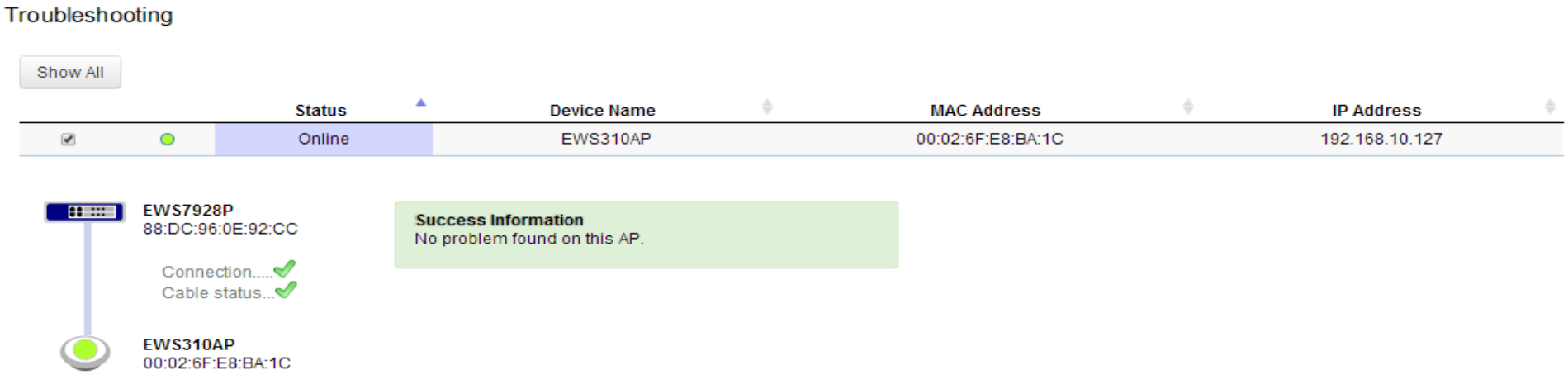
Choosing an Access Point to Diagnose

The list will show the current status of Access Points on the network. Select an Access Point to begin a diagnostic test. If multiple Access Points are connected, use the search bar to the top right of the page to find the Access Point you wish to troubleshoot.



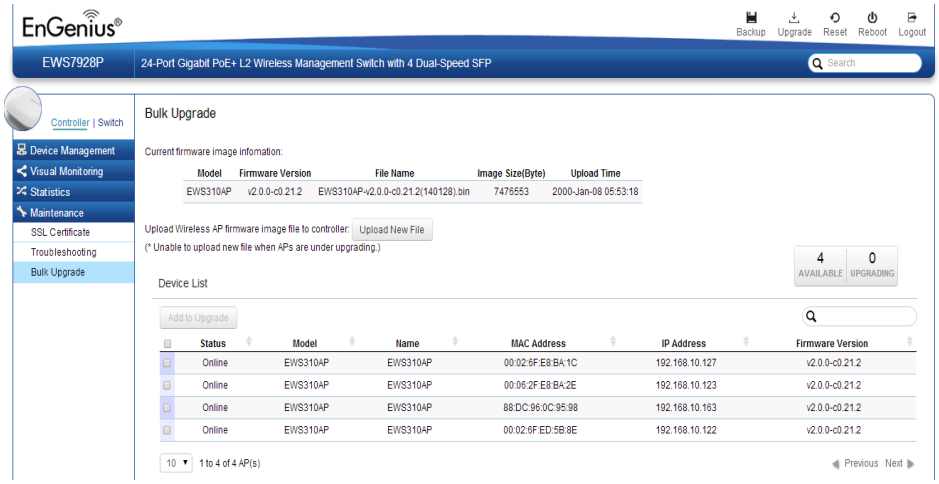
The controller will run a diagnostic test for the selected Access Point. Click **Start** to run the test. The test take a few minutes to complete. Afterwards, the results will display on the page.





Bulk Upgrade

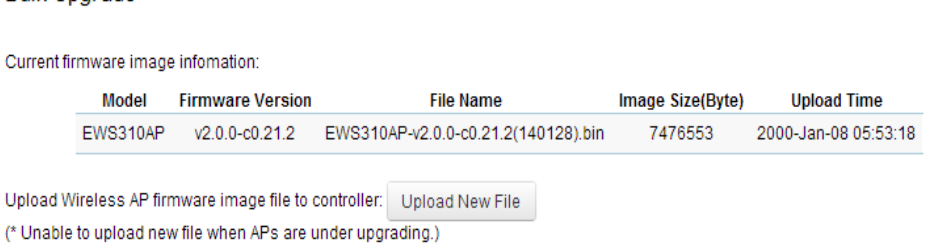
The Bulk Upgrade feature allows administrators to upgrade the firmware of multiple Aaccess Points at the same time. After selecting **Bulk Upgrade** under **Maintenance**, the page will display devices that are available to currently upgrade. Click **Upload New File** to search for new firmware for the device(s).



Model:	Displays the model number of the Access Point.
Firmware Version:	Displays the current firmware version in use.
File Name:	Displays the file name of the firmware uploaded.
Image Size:	Displays the size of the firmware uploaded in bytes.
Upload Time:	Displays the time at which the firmware was uploaded.

Device List

This list displays all the current Access Points connected to the controller. Click on the Access Points you wish to upgrade. If multiple Access Points are connected, you can search for specific Access Points via the search bar at the boittom right of the page. Click **Add to Upgrade** to select devices you wish to upgrade.



Status:	Displays the current status of the Access Point.
Model:	Displays the model number of the Access Point.
Name:	Displays the name of the Access Point.
MAC Address:	Displays the MAC address of the Access Point.
IP Address:	Displays the IP address of the Access Point.
Firmware Version:	Displays the current firmware version of the Access Point.

To upgrade, please follow the steps below:

1. Click on **Upload New File** to mount AP firmware onto EWS Switch flash

2. Once the Access Point firmware is downloaded onto the Controller, the list of Access Points that were selected for the firmware upgrade will appear under **Device List**.

3. Select the Access Points you wish to upgrade and click **Add to Upgrade** to start the firmware upgrading process.

Chapter 3
Switch Management

System

The navigation pane at the left of the Web browser interface contains a System tab that enables you to manage your Switch and controller with features under the following main menu options:

Switch

- "System"
- "L2 Features"
- "VLAN"
- "Management"
- "ACL"
- "QoS"
- "Security"
- "Monitoring"
- "Diagnostics"

Controller

- "Device Management"
- "Visual Monitoring"
- "Statistics"
- "Maintenance"

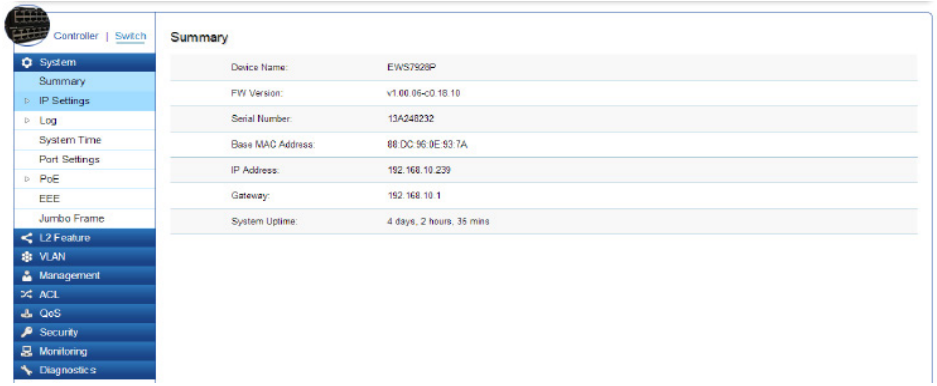
The description that follows in this chapter describes configuring and managing the system settings within the Switch.

Search Bar

At the top right corner of the Graphical User Interface (GUI) is the search bar which you can use to find and jump to any of the Switch or Controller management features. When you type in a word, all possible results for that word in the navigation pane will appear. Click on the results from the drop down list to open that management tab.

Summary

The Summary screen contains general device information about the Switch, including the device name, Firmware version, MAC address, IP address, Gateway, and System Uptime.



Device Name:	Displays the model name of the Switch.
FW version:	Displays the installed firmware version of the Switch.
Serial Number:	Displays the serial number of the Switch.
Base MAC address:	Displays the MAC address of the device.
IP Address:	Displays the IP address assigned by DHCP server.
Gateway:	Displays the Gateway of IP interface.
System Uptime:	Displays the amount of time since the most recent device reset. The System Time is displayed in the following format: days, hours, and minutes. For example, the display will read: 3 days, 6 hours, 10 minutes.

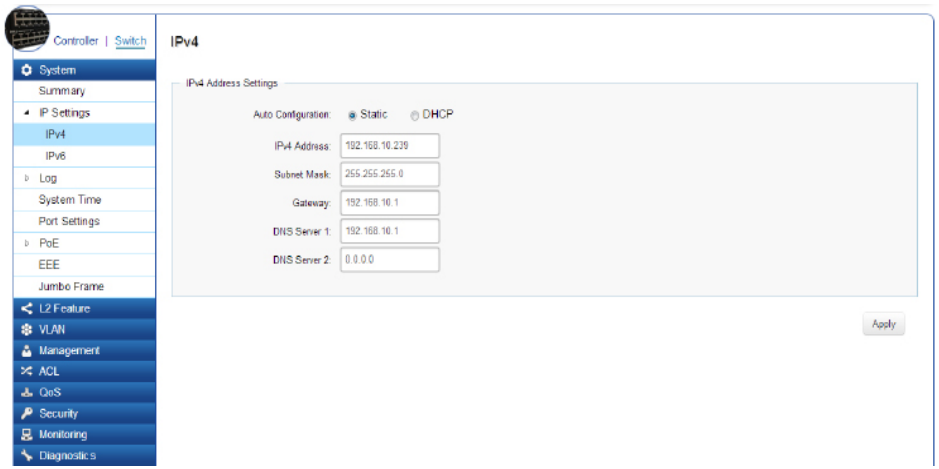
IP Settings

The IP Setting screen contains fields for assigning IP addresses. IP addresses are either defined as static or are retrieved using the Dynamic Host Configuration Protocol (DHCP). DHCP assigns dynamic IP addresses to devices on a network. DHCP ensures that network devices can have a different IP address every time the device connects to the network.

Note the following when configuring IP Addresses:

If the device fails to retrieve an IP address through DHCP, the default IP address is **192.168.0.239**.

To access the page, click **IP Settings** under the **System** menu.



IPv4

To be managed over the network, the Switch needs an IP Address to be assigned. The IP Settings screen contains fields for assigning IP addresses. IP addresses are either defined as Static or are retrieved using the Dynamic Host Configuration Protocol (DHCP). DHCP assigns dynamic IP addresses to devices on a network. DHCP ensures that network devices have a different IP address every time the device connects to the network.

To access the page, click **IPv4** under **IP Settings** in the **System** menu.

Select whether to you wish to enable **Static** or **DHCP** for Auto-Configuration. Next, enter the information for the IP address, gateway, and DNS servers.

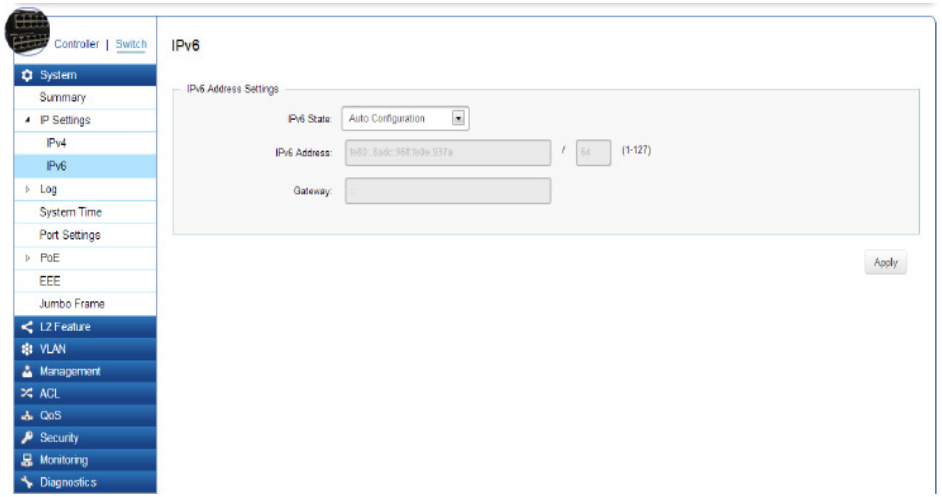
Important: If the device fails to retrieve an IP address through DHCP, then the default IP address is: **192.168.0.239** and the factory default Subnet mask is: **255.255.255.0**.

Dynamic IP Address (DHCP):	Enables the IP address to be configured automatically by the DHCP server. Select this option if you have a DHCP server that can assign the Switch an IP address, subnet mask, default gateway IP address, and a domain name server IP address automatically. Selecting this field disables the IP Address, Subnet mask, and Gateway fields.
Static IP Address:	Allows the entry of an IP address, subnet mask, and a default gateway for the Switch. Select this option if you don't have a DHCP server or if you wish to assign a static IP address to the Switch.
IP Address:	This field allows the entry of an IPv4 address to be assigned to this IP interface. Enter the IP address of your Switch in dotted decimal notation. The factory default value is: **192.168.0.239**.
Subnet Mask:	A Bitmask that determines the extent of the subnet that the Switch is on. This should be labeled in the form: xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimals) between 0 and 255. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed. Enter the IP subnet mask of your Switch in dotted decimal notation. The factory default value is: **255.255.255.0**.
Gateway:	Enter an IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an Intranet, or you do not want the Switch to be accessible outside your local network, you can leave this field blank.
DNS Server (Domain Name System):	Used for mapping a domain name to its corresponding IP address and vice versa. Enter a DNS IP address in order to be able to use a domain name to access the Switch instead of using an IP address.

Apply: Click **APPLY** to update the the system settings.

IPv6

IPv6 is a an upgraded version to IPv4, providing more available IP addresses as well as other benefits. To access the Switch over an IPv6 network, you must first configure it with IPv6 information (IPv6 prefix, prefix length, and default gateway). To configure IPv6 for the Switch, select whether to you wish to enable **Auto-Configuration**, **Static,** or **DHCP** for the IPv6 State. Next, enter the information for the IP address, range, and gateway.



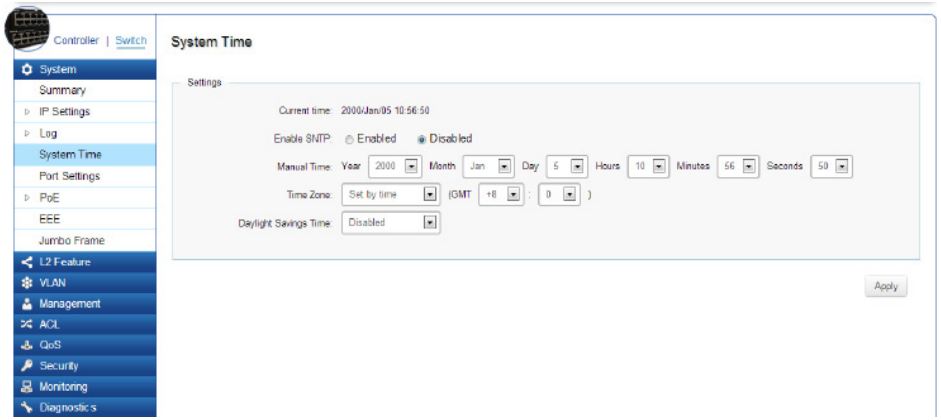
IPv6 State:	Select whether you wish to enable Auto Configuration, DHCPv6 Client, or Static for the IPv6 address.
Auto Configuration:	Use this option to set the IPv6 address for the IPv6 network interface in Auto Configuration. The Switch will automatically generate and use a globally-unique IPv6 address based on the network prefix and its Ethernet MAC address.
DHCPv6 Client:	This enables the IP address to be configured automatically by the DHCP server. Select this option if you have an IPv6 DHCP server that can assign the Switch an IPv6 address/Prefix and a default gateway IP address.
Static:	Allows the entry of an IPv6 address/Prefix and a default gateway for the Switch. Select this option if you wish to assign static IPv6 address information to the Switch.
IPv6 Address:	This field allows the entry of an IPv6 address/Prefix to be assigned to this IP interface.
Gateway:	Set the default gateway IPv6 address for the interface. Enter the default gateway IPv6 address.

Apply: Click **APPLY** to update the system settings.

System Time

Use the System Time screen to view and adjust date and time settings.

The Switch supports Simple Network Time Protocol (SNTP). SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. This software operates only as an SNTP client and cannot provide time services to other systems.



Current time:	Displays the current time.
Enable SNTP:	Select whether to **Enable** or **Disable** the SNTP server. The system time is set via an SNTP sever.
Time Zone:	Select the difference between Greenwich Mean Time (GMT) and local time.
Daylight Savings Time:	Select between **Recurring** or **Non-recurring**.
Daylight Savings Time Offset:	Enter the time of Daylight Savings Time Offset.
Recurring From:	Select the Day, Week, Month, and Hour from the list.
Recurring To:	Select the Day, Week, Month, and Hour from the list.
SNTP/NTP Server Address:	Enter the SNTP or NTP sever IP address or hostname.
Server Port:	Displays the time sever port.

To configure date/time through SNMP:

1. Next to the Enable SNTP, select **Enable**.

2. In the Time Zone Offset list, select by country or by the Coordinated Universal Time (UTC/GMT) time zone in which the Switch is located.

3. Next select **Disabled**, **Recurring**, or **Non-Recurring** for Daylight Savings Time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.

4. In the SNTP/NTP Server Address field, enter the IP address or the host name of the SNTP/NTP server.

5. Finally, enter the port number on the SNTP server to which SNTP requests are sent. The valid range is from 1-65535. The default is: 123.

6. Click **APPLY** to update the system settings.

To configure date/time manually:

1. Next to the Enable SNTP, select **Disable**.

2. In the Manual Time field, use the drop-down boxes to manually select the date and time you wish to set.

3. In the Time Zone Offset list, select by country or by the Coordinated Universal Time (UTC/GMT) time zone in which the Switch is located.

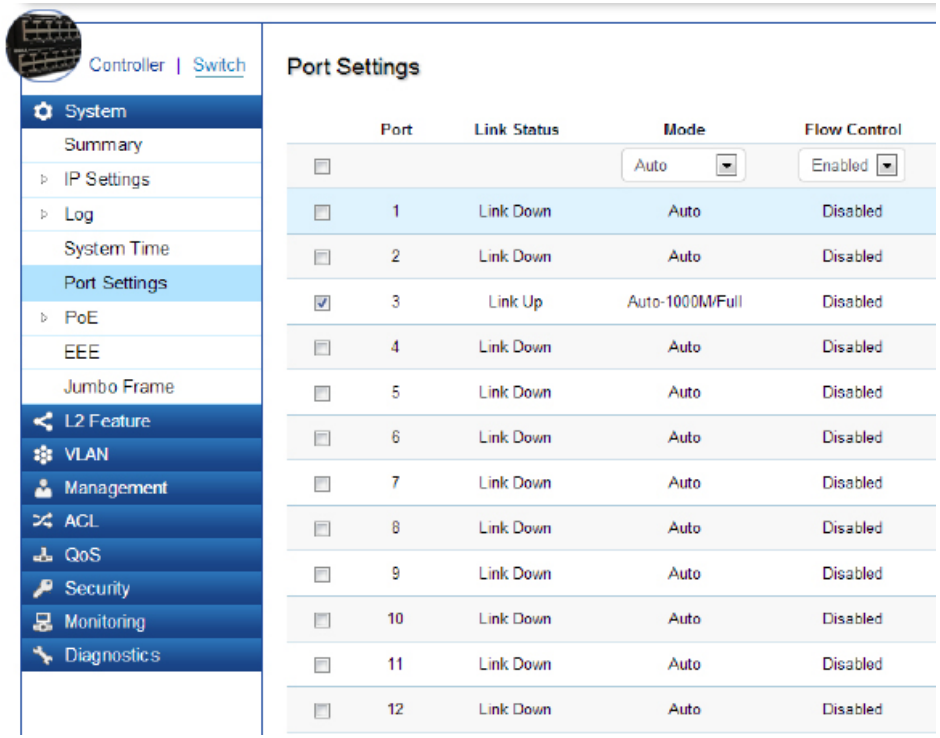
4. Next select **Disabled**, **Recurring** or **Non-recurring** for Daylight Savings Time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.

5. Click **APPLY** to update the system settings.

Port Settings

Use this screen to view and configure Switch port settings. The Port Settings feature lets you change the configuration of the ports on the Switch in order to find the best balance of speed and flow control according to your preferences. Configuring Gigabit ports require additional factors to be considered when arranging your preferences for the Switch compared to 10/100 ports.

To access the page, click **Port Settings** under the **System** menu.



Port:	Displays the port number.
Link Status:	Indicates whether the link is up or down.
Mode:	Select the speed and the duplex mode of the Ethernet connection on this port. Selecting Auto (Auto-Negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support autoegotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.

Flow Control:	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port. The Switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later.

Click **APPLY** to update the system settings.

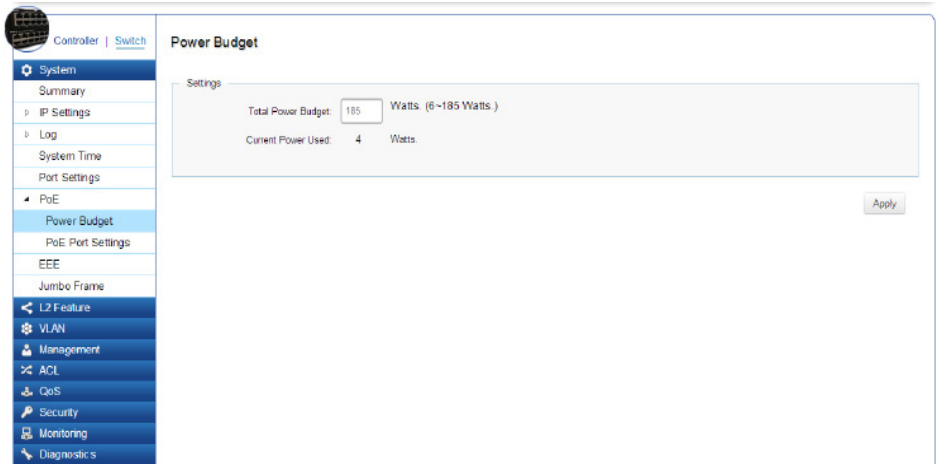
PoE

Power Budget

The PoE Management screen contains system PoE information for monitoring the current power usage and assigns the total amount of power the Switch can provide to all of its PoE ports. Ports 1~8, 24, or 48 on the Switch are IEEE802.3at/af compliant ports. Each port is capable of delivering up to 30 Watts and a total PoE budget of 130, 185, 370, or 740 Watts depending on you model for uninterrupted PoE use. To access the page, click **PoE** under the **System** menu.

	Ports	Power Budget
EWS5912FP	8	130 Watts
EWS7228P	24	185 Watts
EWS7952FP	48	740 Watts

Total Power Budget:	Enter the amount of power the Switch can provide to all ports.
Consumed Power:	Shows the total amount of power currently being delivered to all ports.



Apply: Click **APPLY** to update the the system settings.

PoE Port Settings

The EnGenius Layer 2 PoE+ Switches supports Power over Ethernet (PoE) as defined by the IEEE 802.3af and 802.3at. All ports can support PoE up to 30W. Ports 1-24 can supply about 48 VDC power to Powered Devices (PDs) over standard UTP Ethernet cables. The Switch follows the standard PSE (Power Sourcing Equipment) pinout, whereby power is sent out over pins 1, 2, 3 and 6.

EGS5212FP: Ports 1-8 supports both IEEE802.3 af and at. The maximum power budget is 130 Watts.

EGS7228P: Ports 1-24 supports both IEEE802.3 af and at. The maximum power budget is 185 Watts.

EGS7228FP: Ports 1-24 supports both IEEE802.3 af and at. The maximum power budget is 370 Watts and 720 Watts when you are using the EnGenius RPS370 external redundant power supply.

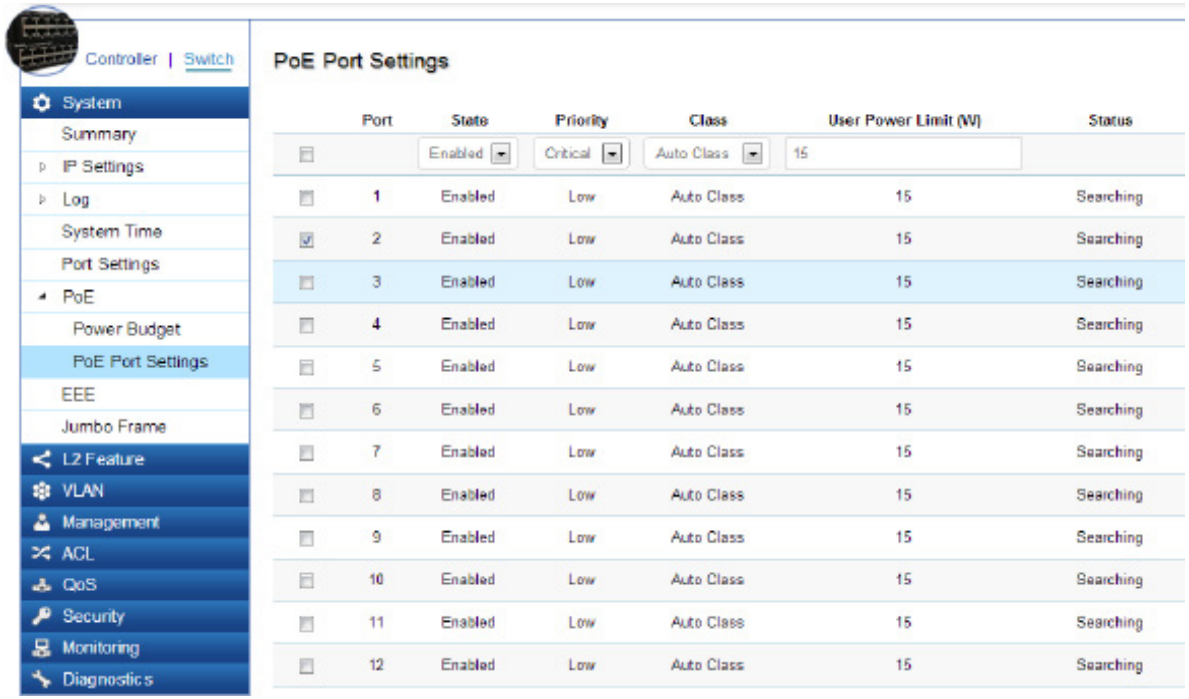
EGS7252FP: Ports 1-48 supports both IEEE802.3 af and at. The maximum power budget is 740 Watts.

To access the page, click **PoE Port Settings** under **PoE** in the **System** Menu.

Port:	Displays the specific port for which PoE parameters are defined. PoE parameters are assigned to the powered device that is connected to the selected port.
State:	• **Enable -** Enables the Device Discovery protocol and provides power to the device using the PoE module. The Device Discovery Protocol lets the device discover powered devices attached to device interfaces and learns their classification. • **Disable -** Disables the Device Discovery protocol and halts the power supply delivering power to the device using the PoE module.
Priority:	Select the port priority if the power supply is low. The field default is **Low**. For example, if the power supply is running at 99% usage, and port 1 is prioritized as high, but port 6 is prioritized as low, port 1 is prioritized to receive power and port 6 may be denied power. The possible field values are: **4**. • **Low** - Sets the PoE priority level as low. • **Medium** - Sets the PoE priority level as medium. • **High** - Sets the PoE priority level as high. • **Critical** - Sets the PoE priority level as critical.

Class(Auto):	Shows the classification of the powered device. The class defines the maximum power that can be provided to the powered device. The possible field values are: • **Class 0** – The maximum power level at the Power Sourcing. Equipment is 15.4 Watts. • **Class 1** – The maximum power level at the Power Sourcing. Equipment is 4.0 Watts. • **Class 2** – The maximum power level at the Power Sourcing. Equipment is 7.0 Watts. • **Class 3** – The maximum power level at the Power Sourcing. Equipment is 15.4 Watts. • **Class 4** – The maximum power level at the Power Sourcing. Equipment is 30 Watts.
Class (User Defined)	Select this option to base the power limit on the value configured in the User Power Limit field.
User Power Limit:	Set the maximum amount of power that can be delivered by a port. **Note:** The User Power Limit can only be implemented when the Class value is set to **User-Defined**.

Status:	Shows the port's PoE status. The possible field values are: • **Delivering Power –** The device is enabled to deliver power via the port. • **Disabled –** The device is disabled for delivering power via the port. • **Test Fail –** The powered device test has failed. For example, a port could not be enabled and cannot be used to deliver power to the powered device. • **Testing -** The powered device is being tested. For example, a powered device is tested to confirm it is receiving power from the power supply. • **Searching –**The device is currently searching for a powered device. Searching is the default PoE operational status. • **Fault –** The device has detected a fault on the powered device when the port is forced on. For example; the power supply voltage is out of range, a short short occurs, a communication or there is a communication errorwith PoE devices, or an unknown error occurs.



Apply: Click **APPLY** to update the the system settings.

EEE

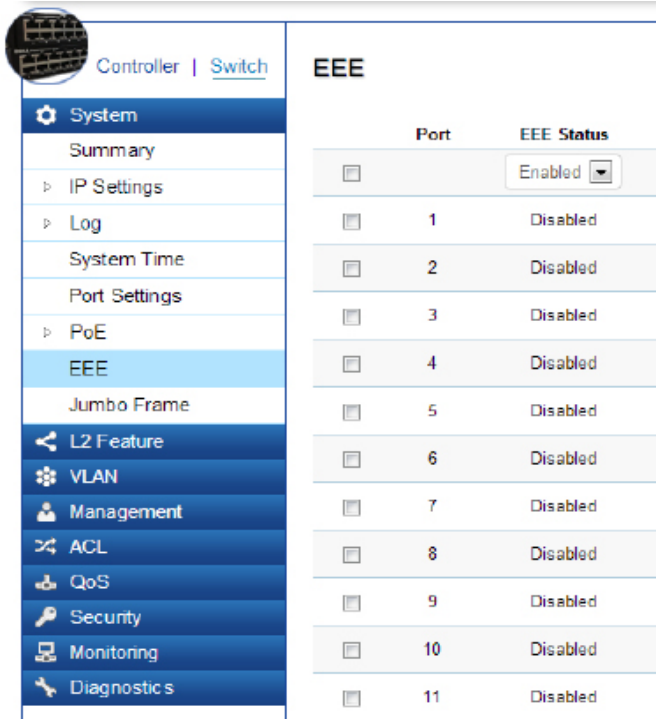
Energy Efficient Ethernet (EEE), an Institute of Electrical and Electronics Engineers (IEEE) 802.3az standard, reduces the power consumption of physical layer devices during periods of low link utilization. EEE saves energy by allowing PHY non-essential circuits shut down when there is no traffic.

Network administrators have long focused on the energy efficiency of their infrastructure, and the EnGenius Layer 2 Switch complies with the IEEE's Energy-Efficient Ethernet (EEE) standard to give you even more control. The EEE-compliant Switch offers users the ability to utilize power that Ethernet links use only during data transmission. Lower Power Idle (LPI) is the method for achieving the power saving during Ethernet idel time.

Use the EEE Configuration page to configure Energy Efficient Ethernet.

Port:	Display the port for which the EEEE setting is displayed.
EEE Status:	**Enable** or **Disable** EEE for the specified port.

Click **APPLY** to update the system settings.



L2 Features

The L2 Feature tab exhibits complete standard-based Layer 2 switching capabilities, including: Link Aggregation, 802.1D single Spanning Tree Protocol, 802.1w Rapid Spanning Tree Protocol, 802.1s Multiple Spanning Tree Protocol, MAC Address Table, Internet Group Management Protocol (IGMP) Snooping, Port Mirroring, 802.1ab Link Layer Discovery Protocol (LLDP), and Multicast Listener Discovery(MLD) snooping. Utilize these features to configure the Switch to your preferences.

Link Aggregation

A Link Aggregation Group (LAG) optimizes port usage by linking a group of ports together to form a single, logical, higher-bandwidth link. Aggregating ports multiplies the bandwidth and increases port flexibility for the Switch. Link Aggregation is most commonly used to link a bandwidth intensive network device (or devices), such as a server, to the backbone of a network.

The participating ports are called Members of a port trunk group. Since all ports of the trunk group must be configured to operate in the same manner, the configuration of the one port of the trunk group is applied to all ports of the trunk group. Thus, you will only need to configure one of any of the ports in a trunk group. A specific data communication packet will always be transmitted over the same port in a trunk group. This ensures the delivery of individual frames of a data communication packet will be received in the correct order. The traffic load of the LAG will be balanced among the ports according to Aggregate Arithmetic. If the connections of one or several ports are broken, the traffic of these ports will be transmitted on the normal ports, so as to guarantee the connection reliability.

When you aggregate ports, the ports and LAG must fulfill the following conditions:

- All ports within a LAG must be the same media/ format type.
- A VLAN is not configured on the port.
- The port is not assigned to another LAG.
- The Auto-negotiation mode is not configured on the port.
- The port is in full-duplex mode.
- All ports in the LAG have the same ingress filter ing and tagged modes.
- All ports in the LAG have the same back pressure and flow control modes.
- All ports in the LAG have the same priority.
- All ports in the LAG have the same transceiver type.
- Ports can be configured as LACP ports only if the ports are not part of a previously configured LAG.

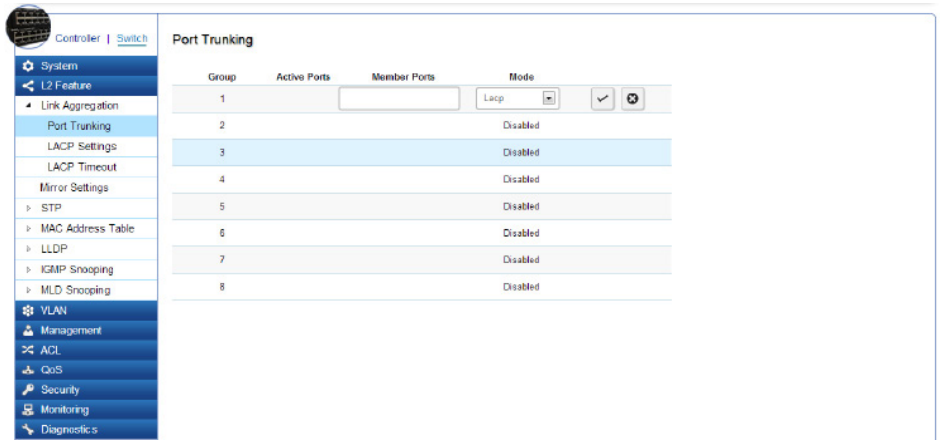
LACP is a dynamic protocol which helps to automate the configuration and maintenance of LAG's. The main purpose of LACP is to automatically configure individual links to an aggregate bundle, while adding new links and helping to recover from link failures if the need arises. LACP can monitor to verify if all the links are connected to the authorized group. LACP is a standard in computer networking, hence LACP should be enabled on the Switch's trunk ports initially in order for both the participating Switches/devices that support the standard, to use it.

Port Trunking

Port Trunking allows you to assign physical links to one logical link that functions as a single, higher-speed link, providing dramatically increased bandwidth. Use Port Trunking to bundle multiple connections and use the combined bandwidth as if it were a single larger "pipe".

Important: You must enable Trunk Mode before you can add a port to a trunk group.

To access the page, click **Port Trunking** under **L2 Features.**



Group:	Displays the number of the given trunk group. You can utilize up to 8 link aggregation groups and each group consisting up to 8 ports on the Switch.
Active Ports:	Displays the active participating members of the trunk group.
Member Port:	Select the ports you wish to add into the trunk group. Up to eight ports per group can be assigned. • **Static** - The Link Aggregation is configured manually for specified trunk group. • **LACP** - The Link Aggregation is configured dynamically for specified trunk group
Mode:	LACP allows for the automatic detection of links in a Port Trunking Group when connected to a LACP-compliant Switch. You will need to ensure both the Switch and device connected to are the same mode in order for them to function, otherwise they will not work. Static configuration is used when connecting to a Switch that does not support LACP.

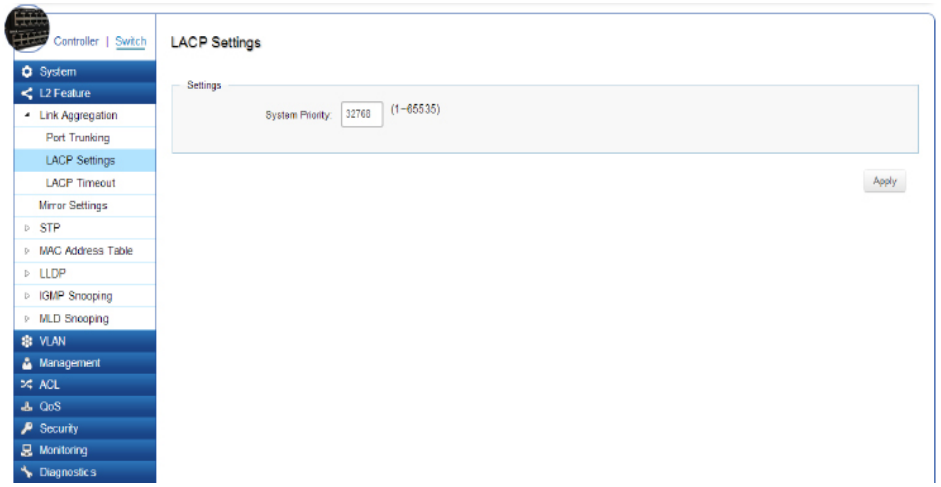
Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Dynamic Link Aggregation: Link Aggregation Control Protocol (LACP)

Link Aggregation Control Protocol (LACP) allows the exchange of information with regard to the link aggregation between the two members of aggregation. This information will be packetized in Link Aggregation Control Protocol Data Units (LACDUs). The trunk group can be configured as an active or passive LACP.

Passive:	The port prefers to not transmit LACPDUs. The port will only transmit LACPDUs when its counterpart uses an active LACP (A preference not to speak unless spoken to).
Active:	The port prefers to transmit LACPDUs, regardless of whether its counterpart uses passive LACP or not (A preference to speak regardless).

LACP (Link Aggregation Control Protocol) Settings



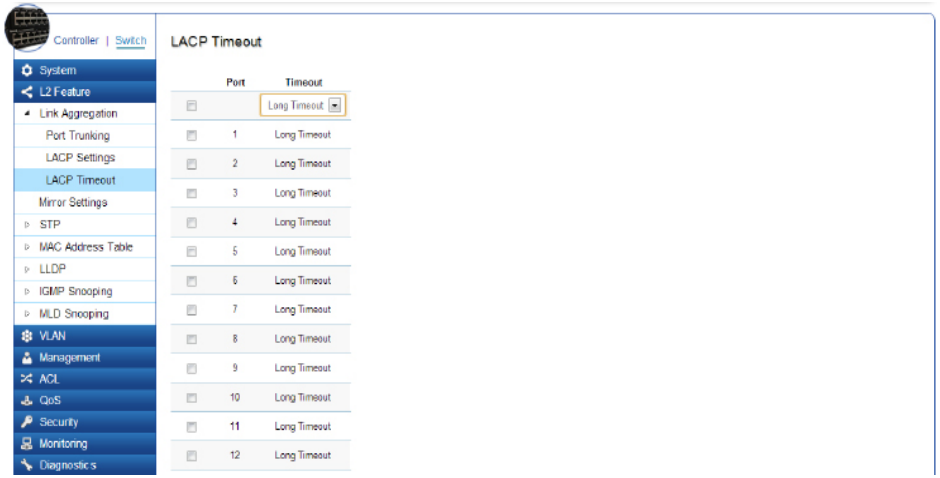
Assign a system priority to run with Link Aggregation Control Protocol (LACP) and is become for a backup link if a link goes down. The lowest system priority is allowed to make decisions about which ports it is actively participating in in case a link goes down. If two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port. If a LAG already exists with the maximum number of allowed port members, and LACP is subsequently enabled on another port using a higher priority than an existing member, the newly configured port will replace the existing port member that has a lower priority. A smaller number indicates a higher priority level. The range is from 0-65535 and default is: 32768.

System Priority:	Enter the LACP priority value to the system. The default is 32768 and the range is from 1-65535.

Apply: Click **APPLY** to update the the system settings.

LACP Timeout

Link Aggregation Control Protocol (LACP) allows the exchange of information with regard to the link aggregation between two members of aggregation. The LACP Time Out value is measured in a periodic interval. Check first whether the port in the trunk group is up. When the interval expires, it will be removed from the trunk. Set a Short Timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. The default value for LACP time out is: Long Timeout.



Timeout:	Select the administrative LACP timeout. • **Long** - Long timeout value. • **Short** - Short timeout value.
Long:	The LACP PDU will be sent for every 30 seconds, and the LACP timeout value is 90 seconds.
Short:	The LACP PDU will be sent every second. The timeout value is 3 seconds.

Apply: Click **APPLY** to update the the system settings.

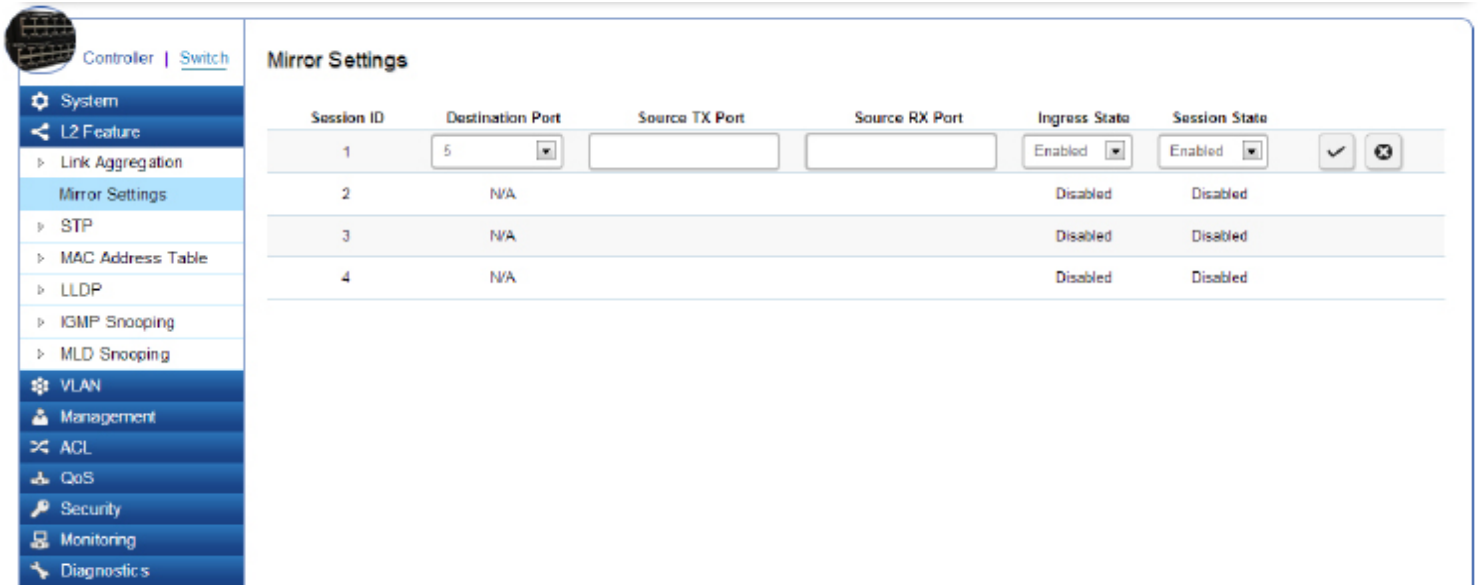
Mirror Settings

Mirrors network traffic by forwarding copies of incoming and outgoing packets from specific ports to a monitoring port. The packet that is copied to the monitoring port will be the same format as the original packet.

Port mirroring is useful for network monitoring and can be used as a diagnostic tool. Use port mirroring to send traffic to applications that analyze traffic for purposes such as monitoring compliance, detecting intrusions, monitoring and predicting traffic patterns, and other correlating events. Port Mirroring is needed for traffic analysis on a Switch because a Switch normally sends packets only to the port to which the destination device is connected. The analyzer captures and evaluates the data without affecting the client on the original port. Port mirroring can consume significant CPU resources while active, so be concious of such usage when configuring the Switch.

Apply: Click **APPLY** to update the the system settings.

Mirror ID:	A number identifying the mirror session. This Switch only supports up to 4 mirror sessions.
Port:	Displays the session ID for port mirroring.
Destination Port:	Select the port for traffic purposes from source ports mirrored to this port.
Source TX/RX Port:	Sets the source port from which traffic will be mirrored. **TX Port:** Only frames transmitted from this port are mirrored to the destination port. **RX Port:** Only frames received on this port are mirrored to the destination port. **Both:** Frames received and transmitted on this port are mirrored to the specified destination port. **None:** Disables mirroring for this port.
Ingress State	Select whether to **Enable** or **Disable** ingress traffic forwarding.
Session State:	Select whether to **Enable** or **Disable** port mirroring.



NOTE: You cannot mirror a faster port onto a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause through-put problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies. Please note a target port and a source port cannot be the same port.

Click the **Apply** button ✓ to accept the changes or the **Cancel** button ⊗ to discard them.

STP

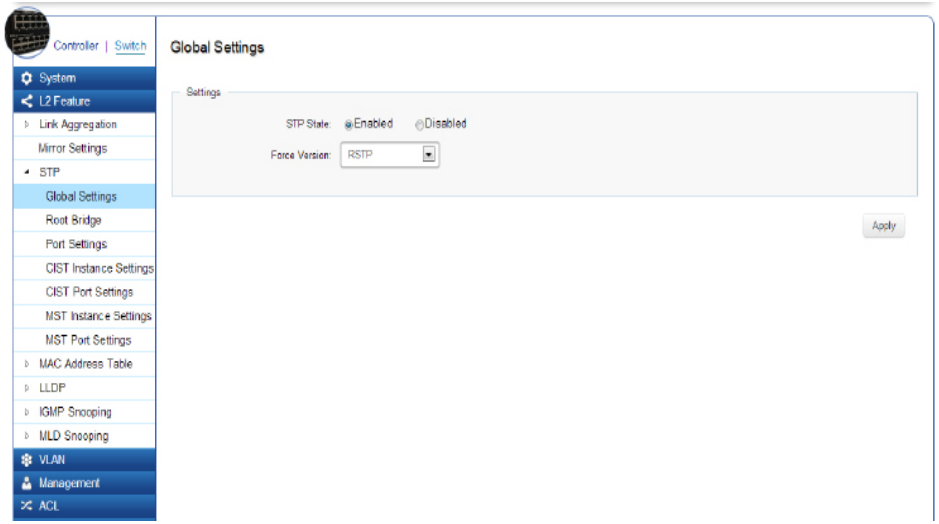
The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between Switches. This allows the Switch to interact with other bridging devices in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

STP provides a tree topology for the Switch. There are different types of Spanning tree verisons, supported, including Spanning Tree Protocol (STP) IEEE802.1D, Multiple Spanning Tree Protocol (MSTP) IEEE802.1w, and Rapid Spanning Tree Protocol (RSTP) IEEE802.1s. Please note that only one spanning tree can be active on the Switch at a time.

STP uses a distributed algorithm to select a bridging device that serves as the root for the spanning tree network. It does this by selecting a root port on each bridging device to incur the lowest path cost when forwarding a packet from that device to the root device. It then selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. Next, all ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, disabling all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops. STP provides a single active path between two devices on a network in order to prevent loops from being formed when the Switch is interconnected via multiple paths.

Global Settings

Spanning Tree Protocol (STP) is a Layer 2 protocol that runs on Switches. Spanning Tree Protocol (STP) allows you to ensure that you do not create loops when you have redundant paths in the network. STP provides a single active path between two devices on a network in order to prevents loops from being formed when the Switch is interconnected via multiple paths.



Once a stable network topology has been established, all bridges listen for Hello Bridge Protocol Data Units (BPDUs) transmitted from the Root Bridge of the Spanning Tree. If a bridge does not receive a Hello BPDU after a predefined interval (known as the Maximum Age), the bridge will assume that the link to the Root Bridge is down and unavailable. This bridge then initiates negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

Spanning Tree Loops

Loops occur when alternate routes exist between hosts. Loops in an extended network can cause the Switch to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency. Once the STP is enabled and configured, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links is also accomplished automatically. STP provides a tree topology and other Spanning tree versions supported include STP, Multiple Spanning Tree Protocol (MSTP), and Rapid Spanning Tree Protocol (RSTP). Please note that only one spanning tree can be active on the Switch at a time. The default setting is: RSTP.

STP:	Select whether to **Enable** or **Disable** the spanning tree operation on the Switch.
Force Version:	Select the Force Protocol Version parameter for the Switch. • **STP** (Spanning Tree Protocol) - IEEE 802.1D. • **RSTP** (Rapid Spanning Tree Protocol) - IEEE 802.1w. • **MSTP** (Multiple Spanning Tree Protocol) - IEEE 802.1s.

Multiple Spanning Tree Protocol (MSTP) defined in IEEE 802.1s, enables multiple VLANs to be mapped to reducethe number of spanning-tree instances needed to support a large number of VLANs. If there is only one VLAN in the network, a single STP works appropriately.

If the network contains more than one VLAN however, the logical network configured by a single STP would work, but it becomes more efficent to use the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs. MSTP (which is based on RSTP for fast convergence) is designed to support independent spanning trees based on VLAN groups. MSTP provides multiple forwarding paths for data traffic and enables load balancing.

STP and RSTP prevent loops from forming by ensuring that only one path exists between the end nodes in your network. RSTP is designed as a general replacement for the slower, legacy STP. RSTP is also incorporated into MSTP. With STP, convergence can take up to a minute to complete in a larger network. This can result in the loss of communication between various parts of the network during the convergence process so STP can subsequently can lose data packets during transmission.

RSTP on the other hand is much faster than STP. It can complete a convergence in seconds, so it greatly diminishes the possible impact the process can have on your network compared to STP. RSTP reduces the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails and retain the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

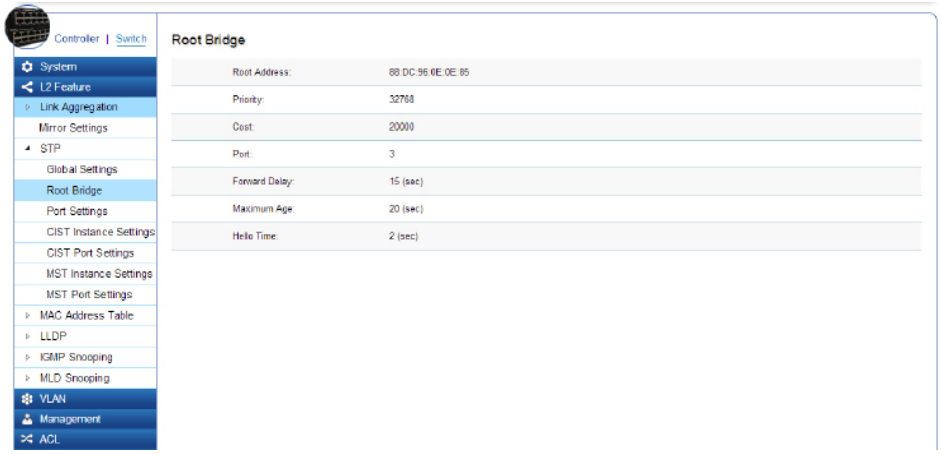
Select whether to **Enable** or **Disable** the Spanning Tree function for the Switch. Next, select whether you wish to enable STP, RSTP, or MSTP. Again, please note that only one Spanning tree function can be active at a time.

Apply: Click **APPLY** to update the the system settings.

Root Bridge

The Root Bridge serves as an administrative point for all Spanning Tree calculations to determine which redundant links to block in order to prevent network loops. From here, you can view all the information regarding the Root Bridge within the STP.

All other decisions in a spanning tree network, such as ports being blocked and ports being put in a forwarding mode, are made regarding a root bridge. The root bridge is the "root" of the constructed "tree" within a spanning tree network. Thus, the root bridge is the bridge with the lowest bridge ID in the spanning tree network. The bridge ID includes two parts; the bridge priority (2 bytes) and the bridge MAC address (6 bytes). The 802.1d default bridge priority is: 32768. STP devices exchange Bridge Protocol Data Units (BPDUs) periodically. All bridges "listen" for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (called the Maximum Age), the bridge assumes that the link to the root bridge is down. The bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

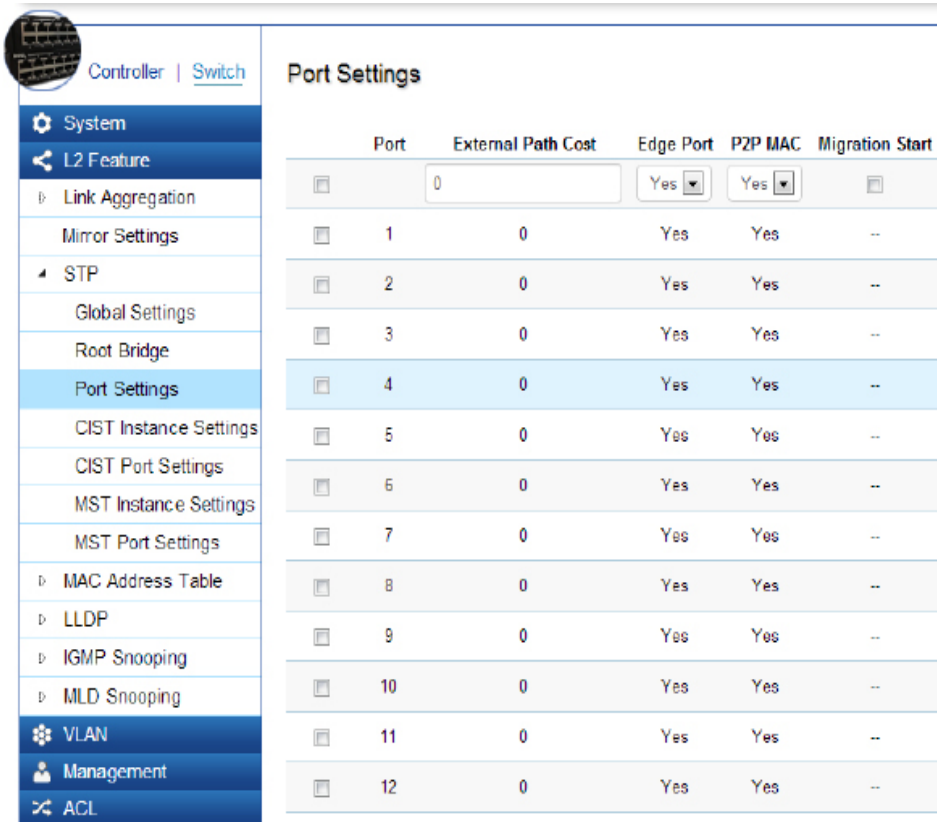


Root Address:	Displays the Root Bridge MAC address. Root in Root Bridge refers to the base of the spanning tree, which the Switch could be configured for.
Priority:	Displays the priority for the bridge. When Switches are running STP, each is assigned a priority. After exchanging BPDUs, the Switch with the lowest priority value becomes the root bridge.
Forward Delay:	Displays the Switch Forward Delay Time. This is the time (in seconds) the Root Switch will wait before changing states (called listening to learning).
Maximum Age:	Displays the bridge Switch Maximum Age Time. This is the amount of time a bridge waits before sending a configuration message. The default is 20 seconds.
Hello Time:	Displays the Switch Hello Time. This is the amount of time a bridge remains in a listening and learning state before forwarding packets. The default is 15 seconds.

Port Settings

STP and RSTP help guard against the formation of loops in an Ethernet network topology. A loop occurs when nodes transmit packets to each other over more than one data path. Packets can become caught in repetitious cycles that needlessly consume network bandwidth which then significantly reduce network performance. With STP, you can set it up on a port per port basis to to further help configure your network topology. The Switch allows each port to have its own spanning tree, and so will require some of its own configuration settings.

Port:	The port or trunked ports you wish to configure.
External Path Cost:	This defines a metric that indicates the relative cost of forwarding packets to the specified port list. The port cost can be set automatically or as a metric value. The default value is 0 (auto). Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. The default port cost for a 100Mbps port is 200000 and the default port cost for a Gigabit port is 20000. Enter a value between 1 and 200000,000 to determine the External Cost. The lower the number, the greater the probability the port will be chosen to forward packets.
Edge Port:	Indicate whether the port is **Enabled** or **Disabled**. •**Yes** - Designates the port as an edge port. • **No** - There is no edge port status.
P2P MAC:	A P2P port must operate in full duplex. Like edge ports, P2P ports transition to a forwarding state rapidly, thus benefiting from RSTP. Enable P2P for the device to establish a point-to-point link, or specify for the device to automatically establish a point-to-point link. Select Yes or No from the list for point-to-point(P2P) . • **Yes** - Restricted in that a P2P port must operate in full-duplex. • **No** -There is no P2P port status.
Migration Start:	When operating in RSTP mode, enable this function to force the port to use the new MST/ RST BPDUs and restart the migration delay timer.

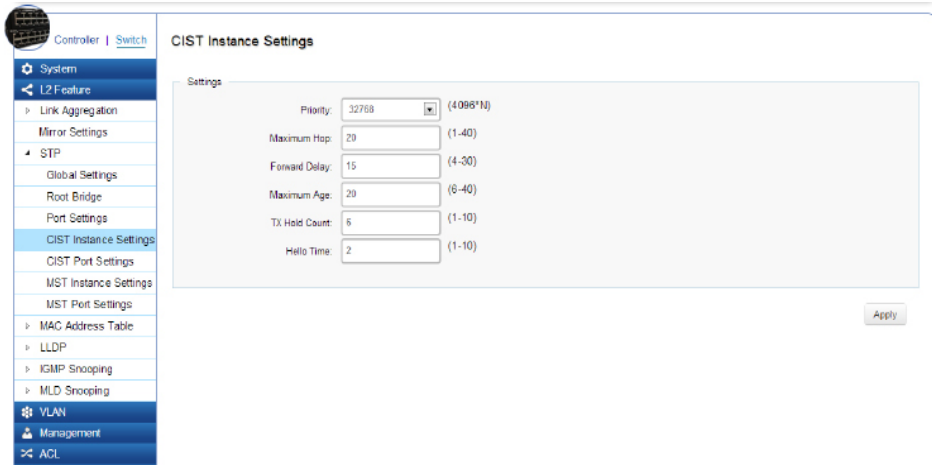


Edge Ports

An edge port changes its initial STP port state from a blocking state to a forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Edge Ports are not connected to LANs that have span¬ning tree devices, so Edge Ports do not receive Bridge Protocol Data Units (BPDUs). If an Edge Port starts to receive BPDUs, it is no longer considered an edge port to the Switch.

Apply: Click **APPLY** to update the the system settings.

CIST Instance Settings



The Common Instance Spanning Tree (CIST) protocol is formed by the spanning-tree algorithm running among bridges that support the IEEE 802.1w, IEEE 802.1s, and IEEE 802.1D standard. A Common and Internal Spanning Tree (CIST) represents the connectivity of the entire network and it is equivalent to a spanning tree in an STP/RSTP.

The CIST inside a Multiple Spanning Tree Instance (MST) region is the same as the CST outside a region. All regions are bound together using a CIST, which is responsible for creating loop-free topology across regions, whereas the MSTI controls topology inside regions. CST instances allow different regions to communicate between themselves. CST is also used for traffic within the region for any VLANs not covered by a MSTI. In an MSTP-enabled network, there is only one CIST that runs between MST regions and single spanning tree devices. A network may contain multiple MST regions and other network segments running RSTP. Multiple regions and other STP bridges are interconnected using a single CST.

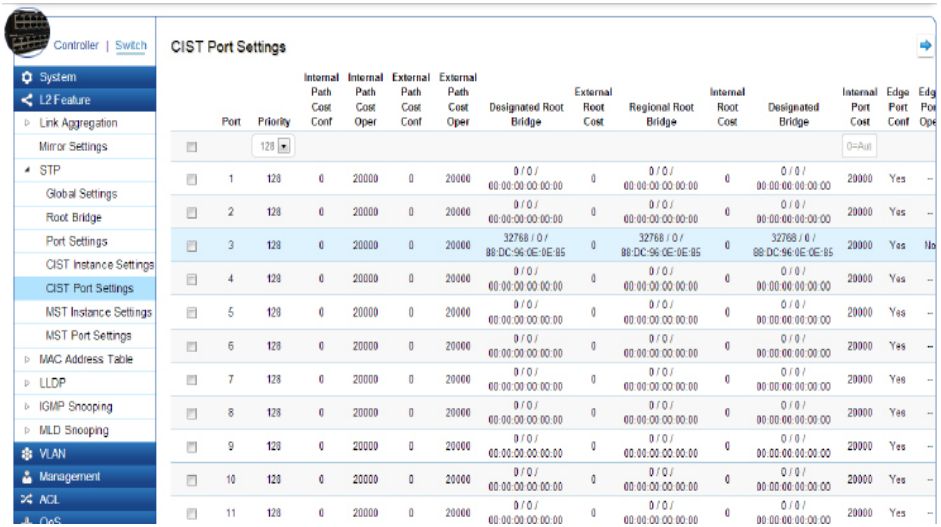
Enter the information to set up CIST for the Switch:

Priority:	Select from the list to specify the priority of the Switch for comparison in the CIST. CIST priority is an important criterion on determining the root bridge. In the same condition, the Switch with the highest priority will be chosen as the root bridge. A lower value has a higher priority. The default value is: 32768 and should be an exact divisor of 4096.
Maximum Hop:	Used to set the number of hops between devices in a spanning tree region before the BPDU packet sent by the Switch is discarded. Each Switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BDPU packet and the information held for the port will age out. The user may set a hop count from 6 to 40. The default value is: 20.
Forward Delay:	Enter the bridge forward delay time, which indicates the amount of time in seconds that a bridge remains in a listening and learning state before forwarding packets. The value must be greater or equal to (Bridge Max Age/2) + 1. The time range is from 4 seconds to 30 seconds. The default value is 15 seconds.
Maximum Age:	The Max Age may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. The user may choose a time between 6 and 40 seconds. The default value is: 20 seconds
TX Hold Count:	Enter the maximum number of Hello packets transmitted per interval. The count can be specified from 1 to 10. The default is: 6.
Hello Time:	Enter the Switch's Hello Time. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to verify that it is the Root Bridge. The Hello Time range is from 1 to 10 seconds. The default Hello Time is: 2 seconds.

Apply: Click **APPLY** to update the the system settings.

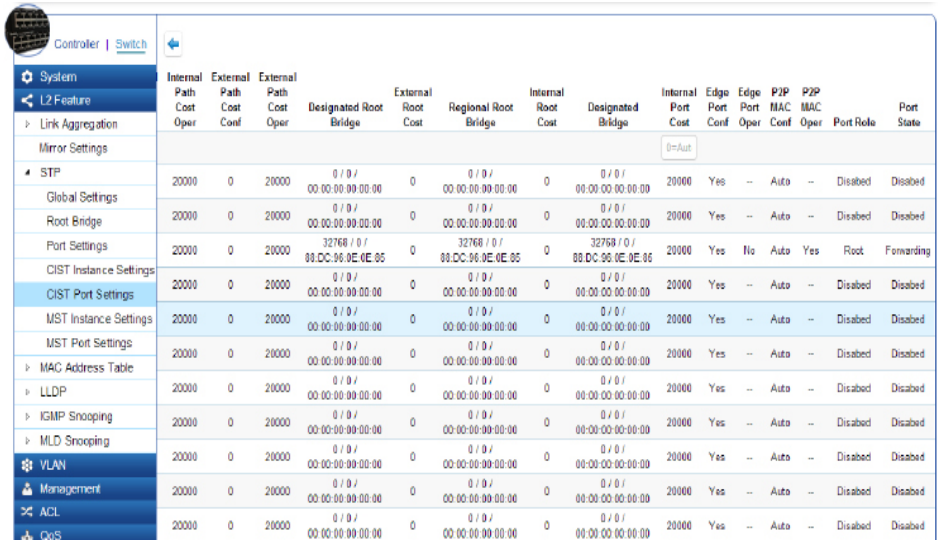
CIST Port Settings

Use the CIST Ports Settings page to configure and view STA attributes for interfaces when the spanning tree mode is set to STP or RSTP. You may use a different priority or path cost for ports of the same media type to indicate a preferred path or Edge Port to indicate if the attached device can support fast forwarding or link type to indicate a point-to-point connection or shared-media connection.



MST ID:	Select the MST ID from the list.
Port:	Port or trunked port identifier.
Priority:	Defines the priority used for this port in the Spanning Tree Algorithm. If the path cost for all ports on a Switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Algorithm is detecting network loops. When more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. The range is from 0-240, in steps of 16; and the default is: 128.
Internal Path Cost Conf:	The Internal Path Cost setting allows you to specify the relative cost of sending spanning tree traffic through the interface to adjacent bridges within a spanning tree region.
Internal Path Cost Oper:	The External Path Cost setting is used to calculate the cost of sending spanning tree traffic through the interface to reach an adjacent spanning tree region. The spanning tree algorithm tries to minimize the total path cost between each point of the tree and the root bridge.

Designated Root Bridge:	Displays the Root Bridge for the CST. It is comprised using the bridge priority and the base MAC address of the bridge.
Internal Root Cost:	This is the cost to the CIST regional root in a region.
External Root Cost:	External Root Cost is the cost to the CIST root.
Regional Root Bridge:	This is the bridge identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.
Internal Port Cost:	Enter the cost of the port.
Edge Port Conf:	Displays the Edge Port state.
Designated Bridge:	This is the Bridge Identifier of the bridge of the Designated Port. It is made up using the bridge priority and the base MAC address of the bridge.
Port Role:	Each MST Bridge Port that is enabled is assigned a Port Role within each spanning tree. The port role will be one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port, or Disabled.
Port State:	The Forwarding State of this port. The state parameters are: Discarding, Learning, Forwarding, or Disabled.



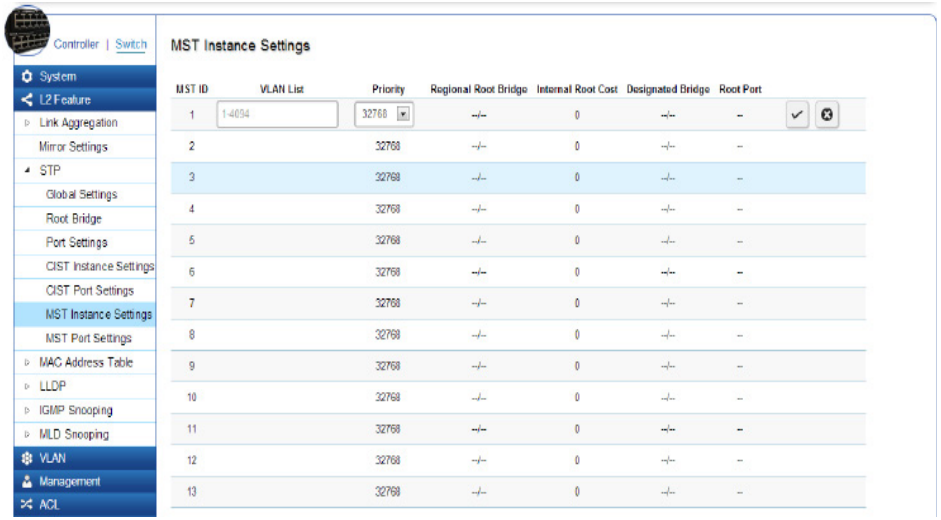
Apply: Click **APPLY** to update the the system settings.

MST Instance Settings

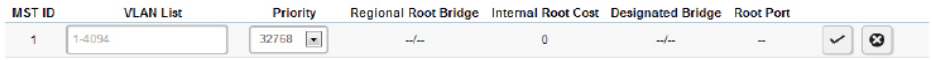
Multiple Spanning Tree Protocol, or MSTP enables the grouping of multiple VLANs with the same topology requirements into one Multiple Spanning Tree Instance (MSTI). MSTP then builds an Internal Spanning Tree (IST) for the region containing commonly configured MSTP bridges. Instances are not supported in STP or RSTP. Instead, they have the same spanning tree in common within the VLAN. MSTP provides the capability to logically divide a Layer 2 network into regions. Every region can contain multiple instances of spanning trees. In MSTP, all of the interconnected bridges that have the same MSTP configuration comprise an MST region.

A Common Spanning Tree (CST) interconnects all adjacent MST Regions and acts as a virtual bridge node for communications between STP or RSTP nodes in the global network. MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of the running spanning tree algorithm between Switches that support STP, RSTP, and MSTP protocols. Once you specify the VLANs you wish to include in a Multiple Spanning Tree Instance (MSTI), the protocol will automatically build an MSTI tree to maintain connectivity among each of the VLANs. MSTP maintains contact with the global network because each instance is treated as an RSTP node in the Common Spanning Tree (CST).

Click the Edit button to configure the MST settings. Next, enter information for the VLAN List and choose the priority you wish to use from the drop-down list.

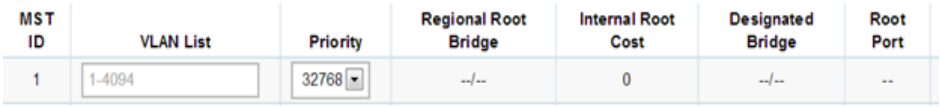


MST ID:	Displays the ID of the MST group that is created. A maximum of 15 groups can be set for the Switch.
VLAN List:	Enter the VLAN ID range from for the configured VLANs to associate with the MST ID. The VLAN ID number range is from 1 to 4094.
Priority:	Select the bridge priority value for the MST. When Switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the Switch with the lowest priority value becomes the root bridge. The default value is: 32768. The range is from 0-61440. The bridge priority is a multiple of 4096.
Regional Root Bridge:	This is the bridge identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.
Internal Root Cost:	Displays the path cost to the designated root for the MST instance.
Designated Bridge:	Displays the bridge identifier of the bridge with the Designated Port. It is made up using the bridge priority and the base MAC address of the bridge.
Root Port:	Displays the port that accesses the designated root for MST instance.
Configuration Name:	This name uniquely identifies the MSTI (Multiple Spanning Tree Instance). Enter a descriptive name (up to 32 characters) for an MST region. The default is the MAC address name of the device running MSTP.
Configuration Reversion:	This value, along with the Configuration Name, identifies the MSTP region configured on the Switch. Devices must have the same revision number to belong to the same region.



Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

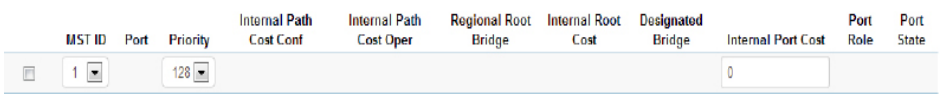
MST ID:	Displays the ID of the MST that is created.
VLAN List:	Enter the VLAN ID to associate with the MST ID.
Priority:	Select the bridge priority value. When Switches or bridges are running STP, each is assigned a priority. The default value is 32768. The range is from 0-61440. The bridge priority value is provided in increments of 4096.
Regional Root Bridge:	Displays the bridge ID for the selected MST instance.
Internal Root Cost:	Displays the path cost to the designated root for the MST instance.
Designated Bridge:	Displays the bridge ID of the root bridge.
Root Port:	Displays the port that accesses the designated root for MST instance.
Configuration Name:	This name uniquely identifies the MSTI (Multiple Spanning Tree Instance). Enter a descriptive name (up to 32 characters) for an MST region. The default is the MAC address name of the device running MSTP.
Configuration Reversion:	This value, along with the Configuration Name, identifies the MSTP region configured on the Switch. Devices must have the same revision number to belong to the same region.



Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

MST Port Settings

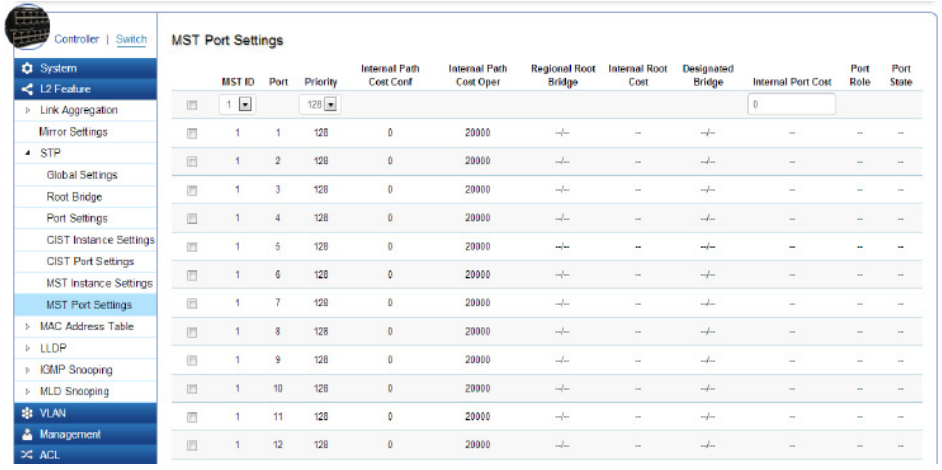
This page displays the current MSTI configuration information for the Switch. From here you can update the port configuration for an MSTI ID. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for ports you wish to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest MAC address into the forwarding state and other interfaces will be blocked. Note that a lower priority values mean higher priorities for forwarding packets.



MST ID:	Displays the ID of the MST group that is created. A maximum of 15 groups can be set for the Switch.
Port:	Displays port or trunked port ID.
Priority:	Select the bridge priority value for the MST. When Switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the Switch with the lowest priority value becomes the root bridge. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example, if you set the priority to any value from 0 through 4095, the priority is set to 0. The default priority is: 32768. The valid range is from 0-61440.
Internal Path Cost Conf:	The Internal Path Cost setting allows you to specify the relative cost of sending spanning tree traffic through the interface to adjacent bridges within a spanning tree region.
Internal Path Cost Oper:	Displays the operation cost of the path from this bridge to the Root Bridge.
Regional Root Bridge:	This is the bridge identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.

Internal Root Cost:	Displays the path cost to the designated root for the selected MST instance.
Designated Bridge:	Displays the Bridge Identifier of the bridge for the Designated Port. It is made up using the bridge priority and the base MAC address of the bridge.
Internal Port Cost:	This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within an STP instance. Selecting this parameter with a value in the range of 1 to 200000000 will set the quickest route when a loop occurs. A lower internal cost represents a quicker transmission. Selecting 0 (zero) for this parameter will set the quickest optimal route automatically for an interface.
Port Role:	Each MST bridge port that is enabled is assigned a Port Role for each spanning tree. The Port Role is one of the following values: Root, Designated, Alternate, Backup, Master, or Disabled.
Port State:	Displays the state of the selected port.
Edge Port Oper:	Displays the operating Edge Port state.
P2P MAC Conf:	Displays the P2P MAC state.
P2P MAC Oper:	Displays the operating P2P MAC state.
Port Role:	Displays the port role. Shows each MST Bridge Port that is assigned a port role for each spanning tree.
Port State:	Displays the state of the selected port.

Port State:	Indicates the current STP state of a port. If enabled, the Port State determines what forwarding action is taken regarding traffic. The possible port states are: • **Disabled:** STP is disabled on the port. The port forwards traffic while learning MAC addresses. • **Blocking:** The port is blocked and cannot be used to forward traffic or learn MAC addresses. • **Listening:** The port is in listening mode. The port cannot forward traffic or learn MAC addresses in this state. • **Learning:** The port is in learning mode. The port cannot forward traffic. However, it can learn new MAC addresses. • **Forwarding:** The port is in forwarding mode. The port can forward traffic and learn new MAC addresses in this state.

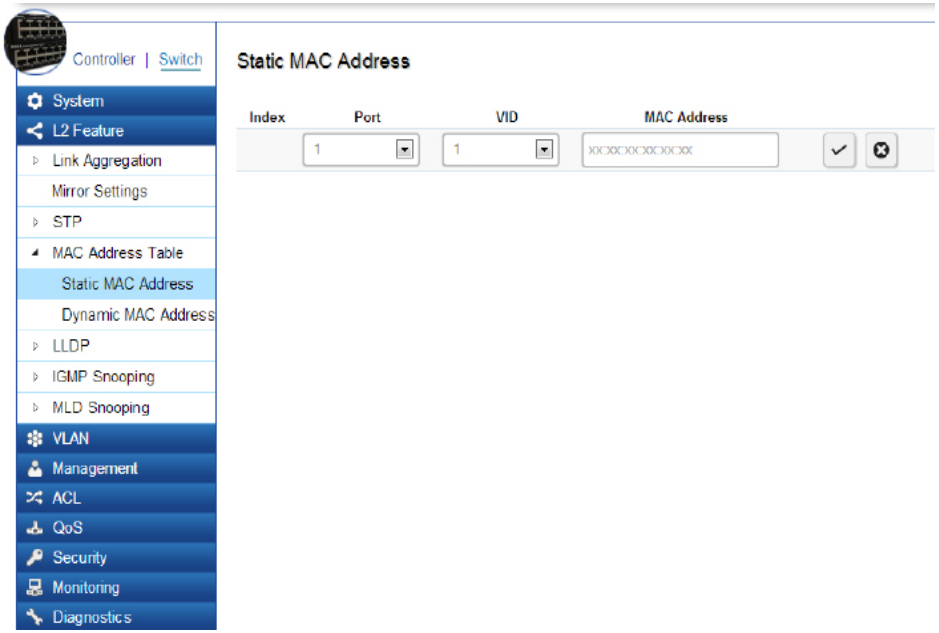


MAC Address Table

The MAC address table contains address information that the Switch uses to forward traffic between the inbound and outbound ports. All MAC addresses in the address table are associated with one or more ports. When the Switch receives traffic on a port, it searches the Ethernet switching table for the MAC address of the destination. If the MAC address is not found, the traffic is flooded out all of the other ports associated with the VLAN. All of the MAC address that the Switch learns by monitoring traffic are stored in the Dynamic address. A Static address allows you to manually enter a MAC address to configure a specific port and VLAN.

Static MAC Address

The address table lists the destination MAC address, the associated VLAN ID, and port number associated with the address. When you specify a Static MAC address, you are set the MAC address to a VLAN and a port; thus it makes an entry into its forwarding table. These entries are then used to forward packets through the Switch. Static MAC addresses along with the Switch's port security allow only devices in the MAC address table on a port to access the Switch.



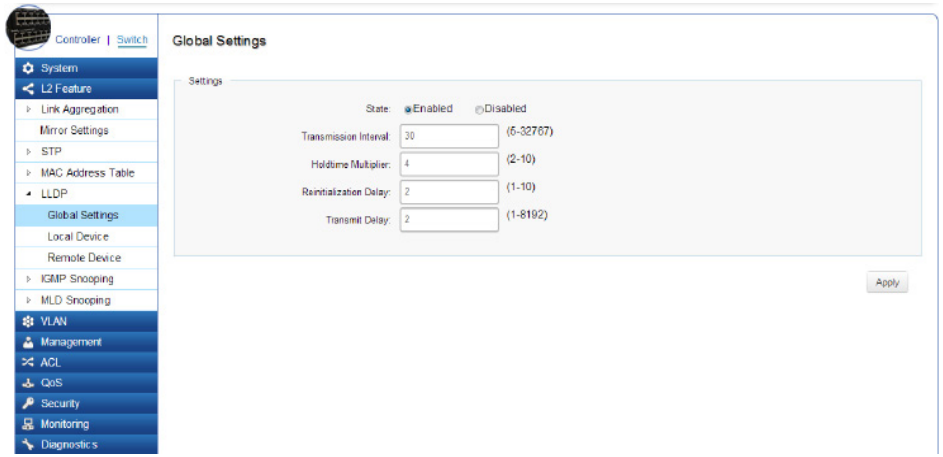
To access the page, click **Static MAC Address** under **L2 Features**.

Index:	Displays the index for the Static MAC Address table.
Port:	Select the port where the MAC address entered in the previous field will be automatically forwarded.
VID:	Enter the VLAN ID on which the IGMP snooping querier is administratively enabled and for which the VLAN exists in the VLAN database.
MAC Address:	Enter a unicast MAC address for which the switch has forwarding or filtering information.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Dynamic MAC Address

The Switch will automatically learn the device's MAC address and store it to the Dynamic MAC address table. If there is no packet received from the device within the aging time, the Switch adopts an aging mechanism for updating the tables from which MAC address entries will be removed from related network devices. The Dynamic MAC Address Table shows the MAC addresses and their associated VLANs learned on the selected port.

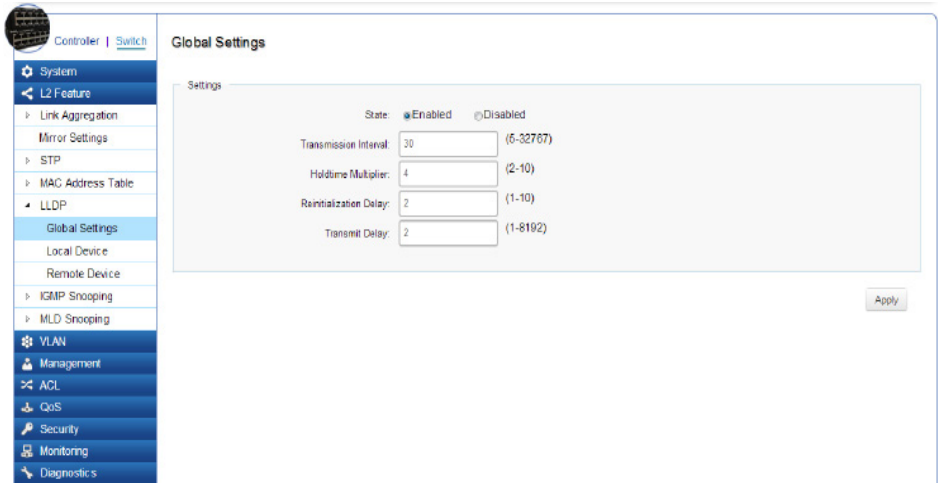


Index:	Displays the index for the Dynamic MAC Address table.
Port:	Select the port to which the entry refers.
VID:	Displays the VLAN ID corresponding to the MAC address.
MAC Address:	Displays the MAC addresses that the Switch learned from a specific port.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

LLDP

Link Layer Discovery Protocol (LLDP) is the IEEE 802.1AB standard for Switches to advertise their identity, major capabilities, and neighbors on the 802 LAN. LLDP allows users to views the discovered information to identify system topology and detect faulty configurations on the LAN. LLDP is essentially a neighbor discovery protocol that uses Ethernet connectivity to advertise information to devices on the same LAN and store information about the network. The information transmitted in LLDP advertisements flow in one direction only; from one device to its neighbors. This information allows the device to quickly identify a variety of other devices, resulting in a LAN that interoperates smoothly and efficiently.



LLDP transmits information as packets called LLDP Data Units (LLDPDUs). A single LLDP Protocol Data Unit (LLDP PDU) is transmitted within a single 802.3 Ethernet frame. A basic LLDPDU consists of a set of Type-Length-Value elements (TLV), each of which contains information about the device. A single LLDPDU contains multiple TLVs. TLVs are short information elements that communicate complex data. Each TLV advertises a single type of information.

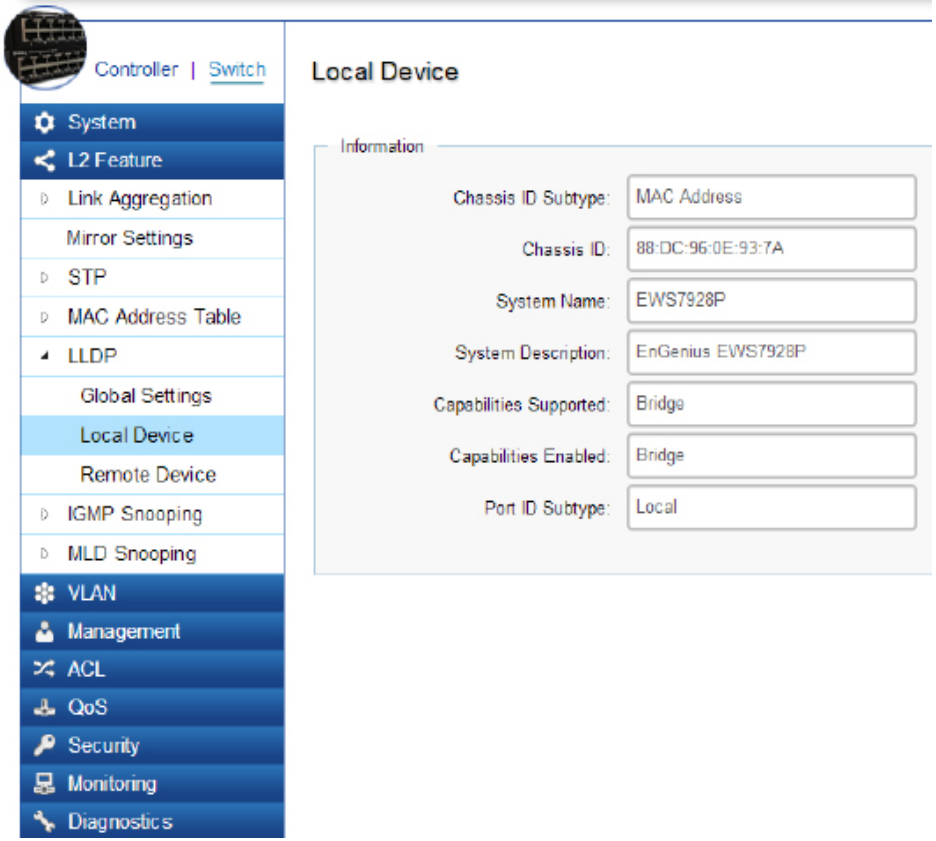
Global Settings

Select whether to **Enable** or **Disable** the LLDP feature on the Switch. Next, enter the Transmission interval, Holdtime Multiplier, Reinitialization Delay parameter, and the Transmit Delay parameter. When finished, click **APPLY** to update the the system settings.

State:	Select **Enabled** or **Disabled** to activate LLDP for the Switch.
Transmission Interval:	Enter the interval at which LLDP advertisement updates are sent. The default value is 30. The range is from 5-32768.
Holdtime Multiplier:	Enter the amount of time that LLDP packets are held before packets are discarded and measured in multiples of the Advertised Interval. The default is 4. The range is from 2-10.
Reinitialization Delay:	Enter the amount of time of delay before reinitializing LLDP. The default is 2. The range is from 1-10.
Transmit Delay:	Enter the amount of time that passes between successive LLDP frame transmissions. The default is 2 seconds. The range is 1-8192 seconds.

Local Device

LLDP devices must support chassis and port ID advertisement, as well as the system name, system ID, system description, and system capability advertisements. Here, you can view detailed LLDP information for the EnGenius Switch.

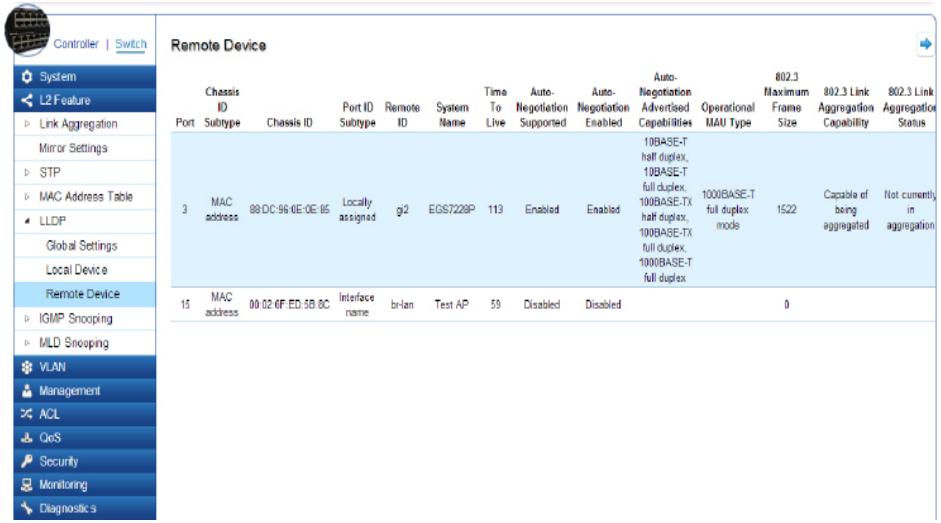


Chassis ID Subtype:	Displays the chassis ID type.
Chassis ID:	Displays the chassis ID of the device transmitting the LLDP frame.
System Name:	Displays the administratively assigned device name.
System Description:	Describes the device.
Capabilities Supported:	Describes the device functions.
Capabilities Enabled:	Describes the device functions.
Port ID Subtype:	Displays the port ID type.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

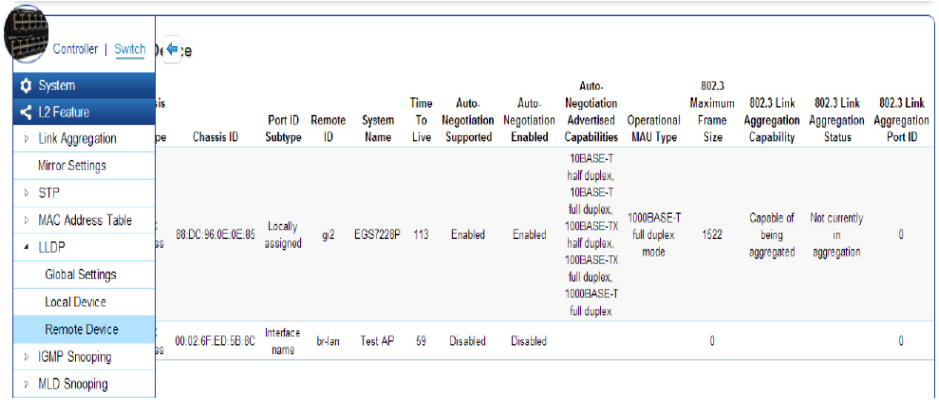
Remote Device

LLDP devices must support chassis and port ID advertisement, as well as the system name, system ID, system description, and system capability advertisements. From here you can viewing detailed LLDP Information for the remote Switch.



Port:	Displays the port.
Chassis ID Subtype:	Displays the chassis ID type.
Chassis ID:	Displays the chassis ID of the device that is transmitting the LLDP frame.
Port ID Subtype:	Displays the port ID type.
Remote ID:	Displays the Remote ID.
System Name:	Displays the administratively assigned device name.
Time to Live:	Displays the time.
Auto-Negotiation Supported:	Displays state for the Auto-Negotiation Supported.
Auto-Negotiation Enabled:	Displays state for the Auto-Negotiation Enabled.
Auto-Negotiation Advertised Capabilities:	Displays the type of Auto-Negotiation Advertised Capabilities.
Operational MAU Type:	Displays the type of MAU.
802.3 Maximum Frame Size:	Displays the size of 802.3 Maximum Frame.
802.3 Link Aggregation Capabilities:	Displays the 802.3 Link Aggregation Capabilities.
802.3 Link Aggregation Status:	Displays the status of 802.3 Link Aggregation.
802.3 Link Aggregation Port ID:	Displays the port ID of 802.3 Link Aggregation.

Mode:	Aggregated links can be set up manually or automatically. Select **Static** or **LACP** for the Link Aggregation type. • **Static** - The Link Aggregation is configured manually for the specified trunk group. • **LACP** - The Link Aggregation is configured dynamically for the specified trunk group.



IGMP Snooping

Internet Group Management Protocol (IGMP) Snooping allows a Switch to forward multicast traffic intelligently. Multicasting is used to support real-time applications such as videoconferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any host that wishes to receive the multicast register with their local multicast Switch.

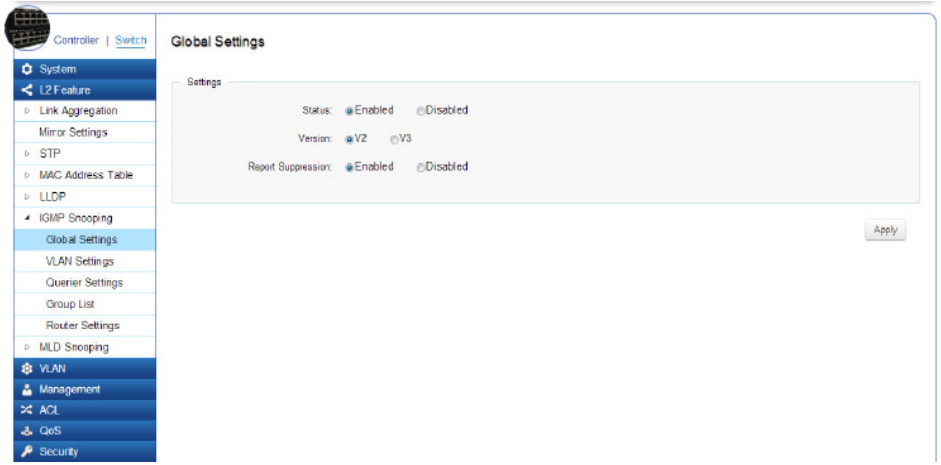
A multicast group is a group of end nodes that want to receive multicast packets from a multicast application. After joining a multicast group, a host node must continue to periodically issue reports to remain a member. Any multicast packets belonging to that multicast group are then forwarded by the Switch from the port.

A Switch supporting IGMP Snooping can passively snoop on IGMP Query, Report, and Leave packets transferred between IP Multicast Switches and IP Multicast hosts to determine the IP Multicast group membership. IGMP Snooping checks IGMP packets passing through the network and configures Multicasting accordingly. Based on the IGMP query and report messages, the Switch forwards traffic only to the ports that request the multicast traffic. It enables the Switch to forward packets of multicast groups to those ports that have validated host nodes. The Switch can also limit flooding of traffic to IGMP designated ports. This improves network performance by restricting the multicast packets only to Switch ports where host nodes are located. IGMP Snooping significantly reduces overall Multicast traffic passing through your Switch. Without IGMP Snooping, Multicast traffic is treated in the same manner as a Broadcast transmission, which forwards packets to all ports on the network.

IGMPv1	Defined in RFC 1112. An explicit join message is sent to the Switch, but a timeout is used to determine when hosts leave a group.
IGMPv2	Defined in RFC 2236. Adds an explicit leave message to the join message so that Switch can more easily determine when a group has no interested listeners on a LAN.
IGMPv3	Defined in RFC 3376. Support for a single source of content for a multicast group.

Global Settings

Click to enable or disable the IGMP Snooping feature for the Switch. Next, select whether you wish to use V2 or V3. Finally, select whether you wish to enable or disable the Report Suppression feature for the Switch.

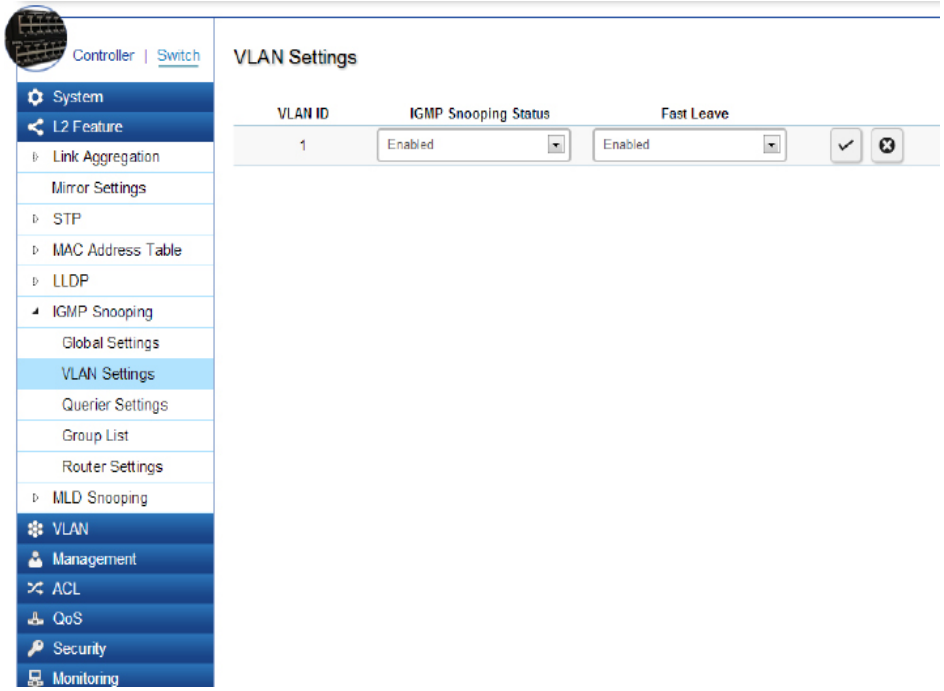


Status:	Select to **Enable** or **Disable** IGMP Snooping on the Switch. The Switch snoops all IGMP packets it receives to determine which segments should receive packets directed to the group address when enabled.
Version:	Select the IGMP version you wish to use. If an IGMP packet received by the interface has a version higher than the specified version, this packet will be dropped.
Report Suppression:	Select whether Report Suppression is **Enabled** or **Disabled** for IGMP Snooping. The Report Suppression feature limits the amount of membership reports the member sends to multicast capable routers.

Apply: Click **Apply** to update the system settings.

VLAN Settings

Use the IGMP Snooping VLAN Settings to configure IGMP Snooping settings for VLANs on the system. The Switch performs IGMP Snooping on VLANs that send IGMP packets. You can specify the VLANs that IGMP Snooping should be performed on.. Choose from the drop-down box whether to **Enable** or **Disable** IGMP Snooping. Next, choose to **Enable** or **Disable** Fast Leave for the VLAN ID.



Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

VLAN ID:	Displays the VLAN ID.
IGMP Snooping Status:	**Enables** or **Disables** the IGMP snooping feature for the specified VLAN ID.
Fast Leave:	**Enables** or **Disables** the IGMP snooping Fast Leave for the specified VLAN ID. Enabling this feature allows the Switch to immediately remove the Layer 2 LAN port from its forwarding table entry upon receiving an IGMP leave message without first sending out IGMP group-specific (GS) queries to the port.

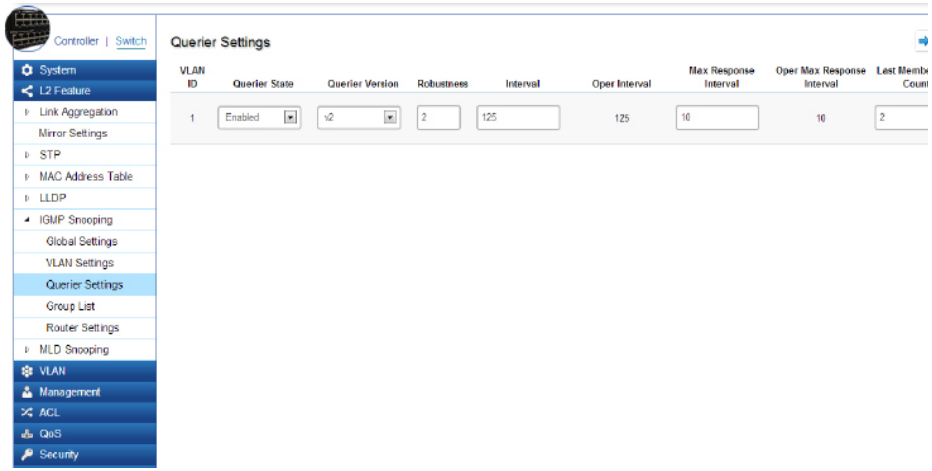
If Fast Leave is not used, a multicast querier will send a GS-query message when an IGMPv2/v3 group leave message is received. The querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period. If Fast Leave is enabled, the Switch assumes that only one host is connected to the port. Therefore, Fast Leave should only be enabled on a port if it is connected to only one IGMP-enabled device.

Fast Leave is supported only with IGMPv2 or IGMPv3 Snooping when IGMP Snooping is enabled. Fast Leave does not apply to a port if the Switch has learned that a multicast querier is attached to it.

Fast Leave can improve bandwidth usage for a network which frequently experiences many IGMP host add and leave requests.

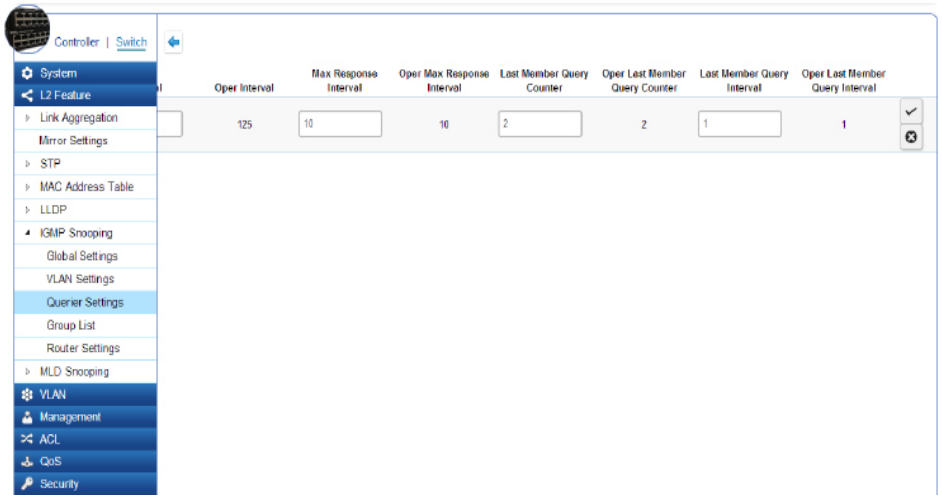
Querier Settings

IGMP snooping requires that one central Switch to periodically query all end devices on the network to announce their Multicast memberships and this central device is the IGMP querier. The snooping Switch sends out periodic queries with a time interval equal to the configured querier query interval. The IGMP query keeps the Switch updated with the current multicast group membership information. If the Switch does not received the updated membership information, then it will stop forwarding multicasts to specified VLANs.



VLAN ID:	Displays the VLAN ID.
Querier State:	Select whether to Enable or Disable the IGMP querier state for the specified VLAN ID. A querier can periodically ask their hosts if they wish to receive multicast traffic. The Querier feature will check whether hosts wish to receive multicast traffic when enabled. An Elected querier will assume the role of querying the LAN for group members, and then propagates the service requests on to any upstream multicast Switch to ensure that it will continue to receive the multicast service. This feature is only supported for IGMPv1 and v2 snooping.
Querier Version:	Enter the version of IGMP packet that will be sent by this port. If an IGMP packet received by the port has a version higher than the specified version, this packet will be dropped.
Robustness:	Provides fine-tuning to allow for expected packet loss on a subnet. It is used in calculating the following IGMP message intervals. The default is 2.
Interval:	Enter the amount of time in seconds between general query transmissions. The default is 125 seconds

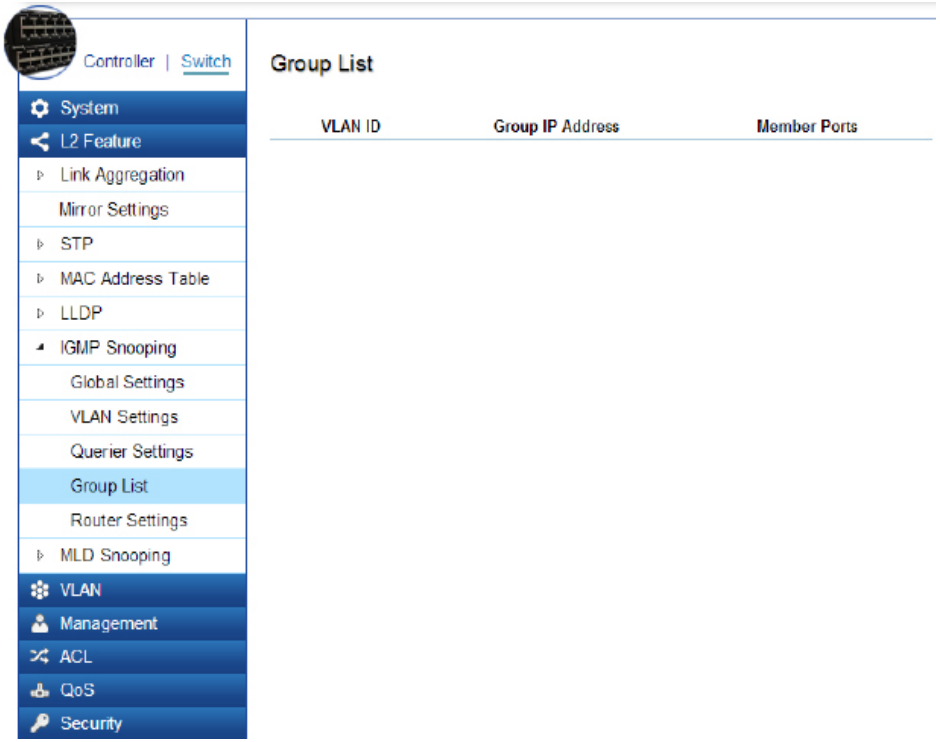
Oper Interval:	Displays the IGMP Interval of the operational querier.
Max Response Interval:	Enter the maximum response time used in the queries that are sent by the snooping querier. The default is 10 seconds.
Oper Max Response Interval:	Display the maximum response time which used in the queries that are sent by the snooping querier.
Last Member Query Counter:	Enter the number of the operational last member querier.
Oper Last Member Query Counter:	Enter the number of IGMP group-specific queries sent before the switch assumes there are no local members.
Last Member Query Interval:	Displays the Operational Last Member Query Interval sent by the elected querier.
Oper Last Member Query Interval:	Enter the time between two consecutive group-specific queries that are sent by the querier, including those sent in response to leave-group messages. You might lower this interval to reduce the amount of time it takes a querier to detect the loss of the last member of a group.



Click the **Apply** button ✓ to accept the changes or the **Cancel** button ⊗ to discard them.

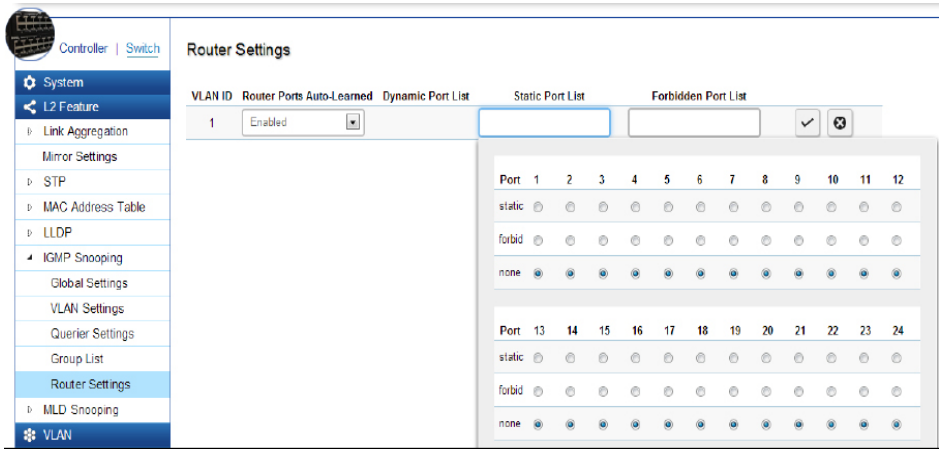
Group List

The Group List displays VLAN ID, Group IP Address, and Members Port in the IGMP Snooping List.



Router Settings

The Router Settings shows the learned multicast router attached port if the port is active and a member of the VLAN. Select the VLAN ID you would like to configure and enter the Static and Forbidden ports for the specified VLAN IDs. All IGMP packets snooped by the Switch will be forwarded to the multicast router reachable from the port.



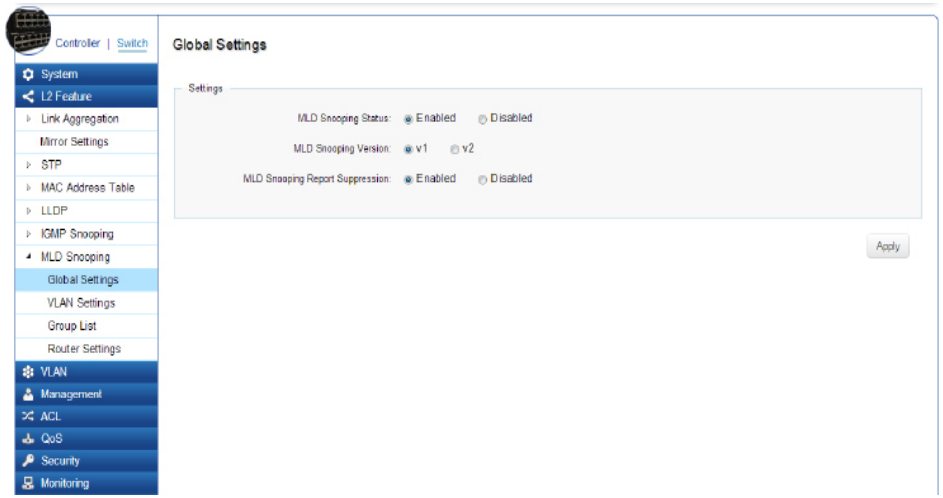
VLAN ID:	Displays the VLAN ID.
Router Ports Auto-Learned:	The Switch will auto detect the prescence of a multicast router and forward IGMP pacets accordingly.
Dynamic Port List:	Displays router ports that have been dynamically configured.
Forbidden Port List:	Designates a range of ports as being disconnected to multicast-enabled routers. Ensures that the forbidden router port will not propagate routing packets out.
Static Port list:	Designates a range of ports as being connected to multicast-enabled routers. Ensures that the all packets will reach the multicast-enabled router

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

MLD Snooping

Multicast Listener Discovery (MLD) Snooping operates on the IPv6 traffic level for discovering multicast listeners on a directly attached port and performs a similar function to IGMP Snooping for IPv4. MLD snooping allows the Switch to examine MLD packets and make forwarding decisions based on content. MLD Snooping limits IPv6 multicast traffic by dynamically configuring the Switch port so that multicast traffic is forwarded only to those ports that wish to receive it. This reduces the flooding of IPv6 multicast packets in the specified VLANs. Both IGMP and MLD Snooping can be active at the same time.

Global Settings

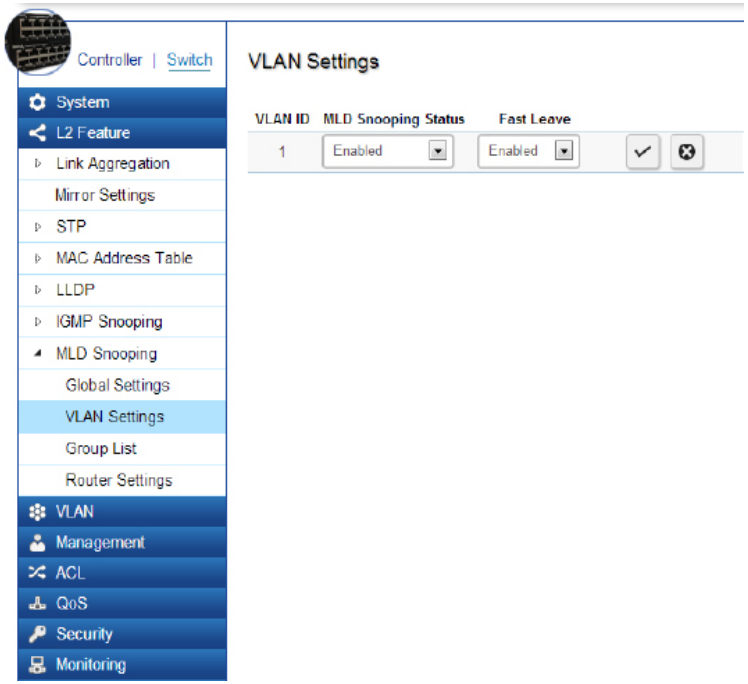


MLD Snooping Status:	Select to **Enable** or **Disable** MLD Snooping on the Switch. The Switch snoops all MLD packets it receives to determine which segments should receive packets directed to the group address when enabled.
MLD Snooping Version:	Select the MLD version you wish to use. If an MLD packet received by the interface has a version higher than the specified version, this packet will be dropped.
MLD Snooping Report Suppression:	The report suppression feature limits the amount of membership reports the member sends to multicast capable routers.

Apply: Click **Apply** to update the system settings.

VLAN Settings

If the Fast Leave feature is not used, a multicast querier will send a GS-query message when an MLD group leave message is received. The querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period. If Fast Leave is enabled, the Switch assumes that only one host is connected to the port. Therefore, Fast Leave should only be enabled on a port if it is connected to only one MLD-enabled device.



Fast Leave does not apply to a port if the Switch has learned that a multicast querier is attached to it.

Fast Leave can improve bandwidth usage for a network which frequently experiences many MLD host add and leave requests.

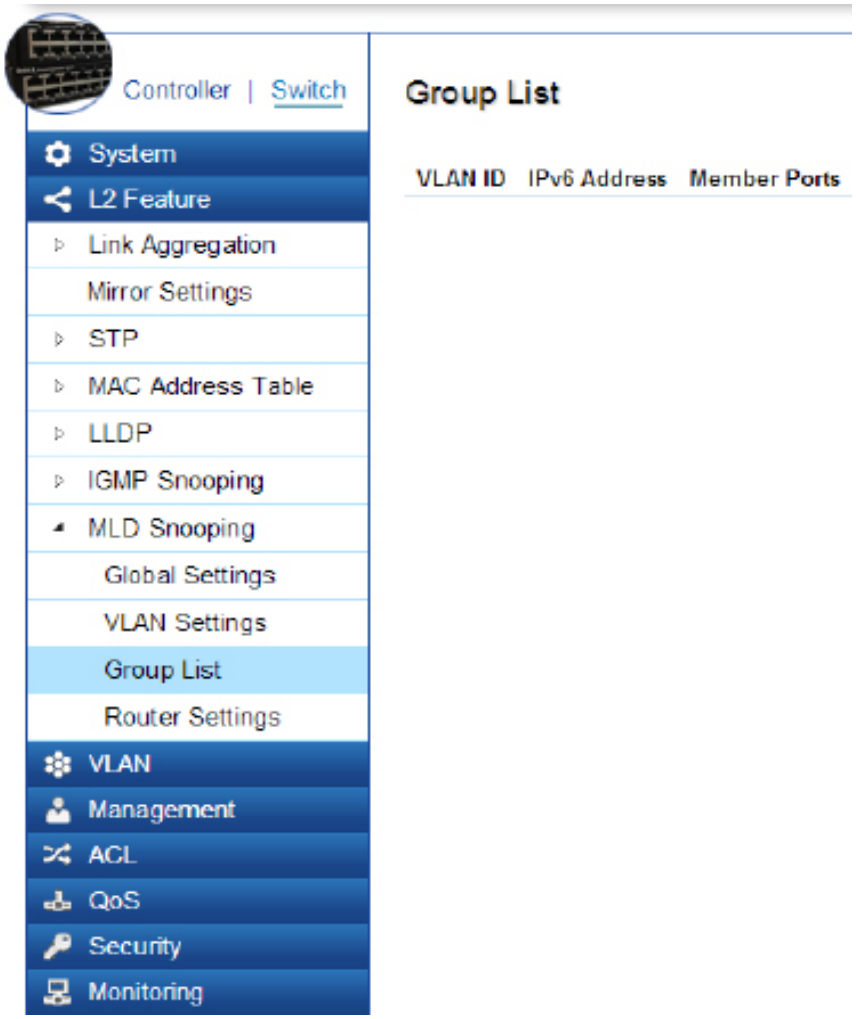
VLAN ID:	Displays the VLAN ID.
MLD Snooping Status:	Select to **Enable** or **Disable** the MLD snooping feature for the specified VLAN ID.
Fast Leave:	Enables or Disables the MLD snooping Fast Leavefeature for the specified VLAN ID. Enabling this feature allows the Switch to immediately remove the Layer 2 LAN port from its forwarding table entry upon receiving an MLD leave message without first sending out an MLD group-specific (GS) query to the port.

Select from the drop-down list whether to **Enable** or **Disable** MLD Snooping. Next, select to **Enable** or **Disable** Fast Leave for the specified VLAN ID.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

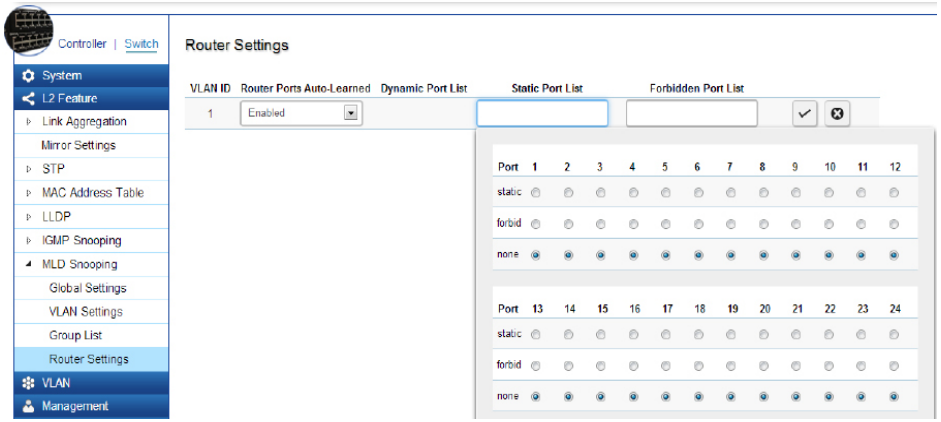
Group List

The Group List displays the VLAN ID, IPv6 Address, and Members Port in the MLD Snooping List.



Router Settings

The Router Settings feature shows the learned multicast router attached port if the port is active and a member of the VLAN. Select the VLAN ID you would like to configure and enter the Static and Forbidden ports for the specified VLAN IDs that are utilizing MLD Snooping. All MLD packets snooped by the Switch will be forwarded to the multicast router reachable from the port.



VLAN ID:	Displays the VLAN ID.
Router Ports Au-to-Learned:	The Switch will automatically detect the presence of a multicast router and forward MLD packets accordingly.
Dynamic Port List:	Displays router ports that have been dynamically configured.
Forbidden Port List:	Designates a range of ports as being dis-connected to multicast-enabled routers. Ensure that the forbidden router port will not propagate routing packets out.
Static Port List:	Designates a range of ports as being connected to multicast-enabled routers. Ensure that the all packets will reach the multicast-enabled router.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

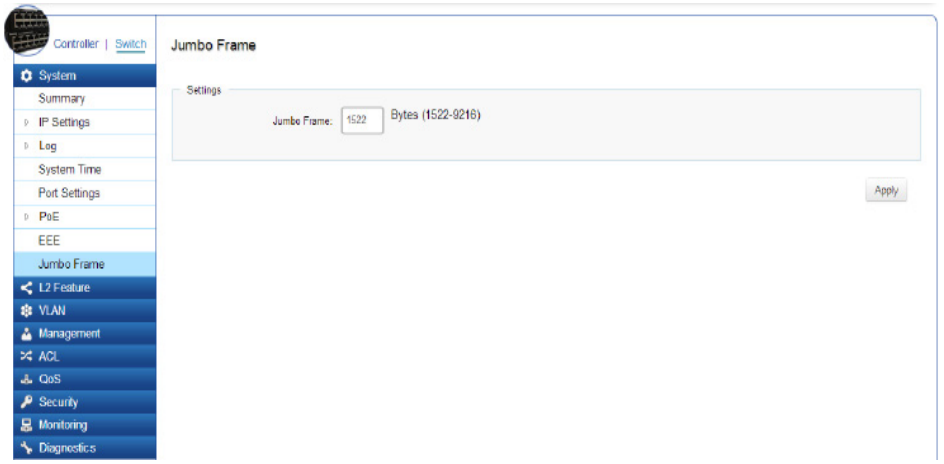
Jumbo Frame

Ethernet has used the 1500 byte frame size since its inception. Jumbo frames are network-layer PDUs that have a size much larger than the typical 1500 byte Ethernet Maximum Transmission Unit (MTU) size. Jumbo frames extend Ethernet to 9000 bytes, making them large enough to carry an 8 KB application datagram plus packet header overhead. If you intend to leave the local area network at high speeds, the dynamics of TCP will require you to use large frame sizes.

The EnGenius Layer 2 Switch supports a Jumbo Frame size of up to 9216 bytes. Jumbo frames need to be configured to work on the ingress and egress port of each device along the end-to-end transmission path. Furthermore, all devices in the network must also be consistent on the maximum Jumbo Frame size, so it is important to do a thorough investigation of all your devices in the communication paths to validate their settings.

Jumbo Frame:	Enter the size of jumbo frame. The range is from 1522-9216 bytes.

Enter the size of jumbo frame. The range is from 1522-9216 bytes. Click **APPLY** to update the the system settings.

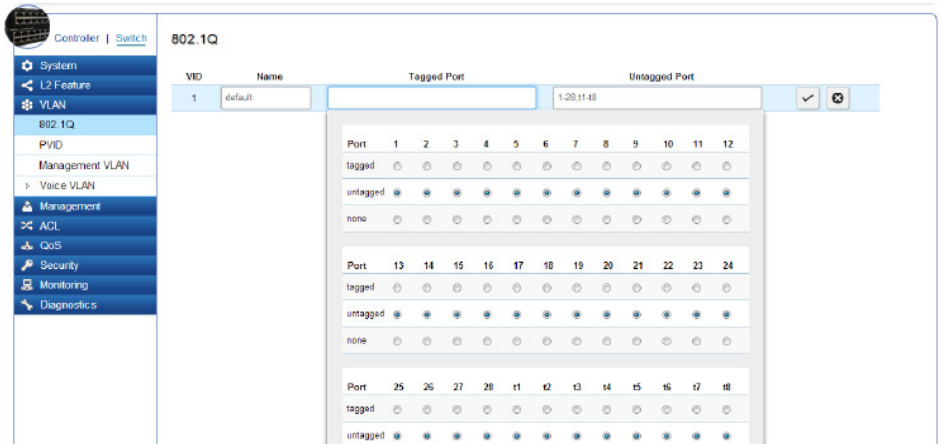


VLAN

A Virtual LAN (VLAN) is a group of ports that form a logical Ethernet segment on a Layer 2 Switch which provides better administration, security, and management of multicast traffic. A VLAN is a network topology configured according to a logical scheme rather than a physical layout. When you use a VLAN, users can be grouped by logical function instead of physical location. All ports that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. VLANs let you logically segment your network into different broadcast domains so that you can group ports with related functions into their own separate, logical LAN segments on the same Switch. This allows broadcast packets to be forwarded only between ports within the VLAN which can avoid broadcast packets being sent to all the ports on a single Switch. A VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. VLANs also improve security by limiting traffic to specific broadcast domains.

802.1Q

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. The IEEE802.1Q specification establishes a standard method for tagging Ethernet frames with VLAN membership information. The key for IEEE802.1Q to perform its functions is in its tags. 802.1Q-compliant Switch ports can be configured to transmit tagged or untagged frames. A tag field containing VLAN information can be inserted into an Ethernet frame. When using 802.1Q VLAN configuration, you configure ports to be a part of a VLAN group. When a port receives data tagged for a VLAN group, the data is discarded unless the port is a member of the VLAN group.



Enabled:	Enables 802.1Q VLANs. This feature is enabled by default.
VID:	Displays the VLAN ID for which the network policy is defined. The range of the VLAN ID is from 1-494.
Name:	Enter the VLAN name. You can use up to 32 alphanumeric characters.
Tagged Port:	Frames transmitted from this port are tagged with the VLAN ID.
Untagged Port:	Frames transmitted from this port are untagged.

Important: Port-based VLAN and 802.1Q VLAN are mutually exclusive. If you enable port-based VLAN, then 802.1Q VLAN is disabled.

Note: The Switch's default setting is to assign all ports to a single 802.1Q VLAN(VID 1). Please keep this in mind when configuring the VLAN settings for the Switch.

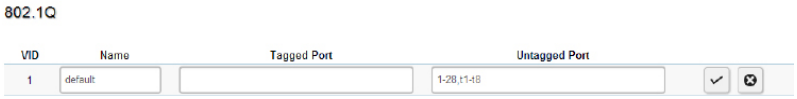
Adding, Editing, and Deleting Items in the List

To add an item to the 802.1Q list, follow these steps:

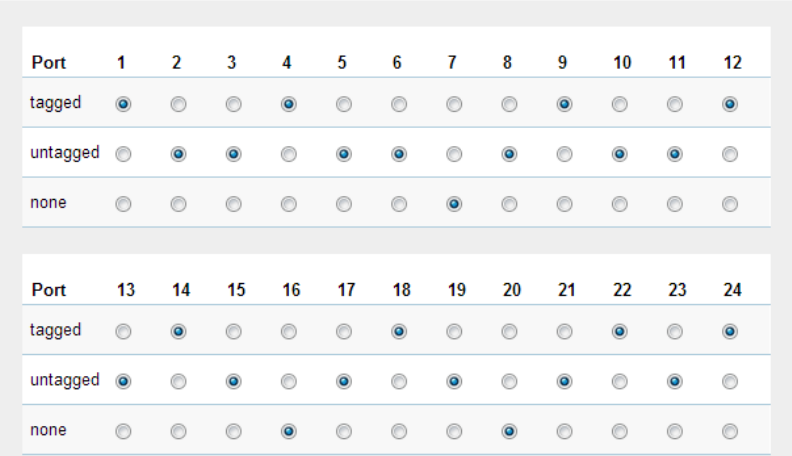
1. Click the **Add** button

.

2. Enter the VID and name in the the **VID** and **Name** text boxes.



3. Click the **Tagged Ports** text box to show the tagged ports dialog box.

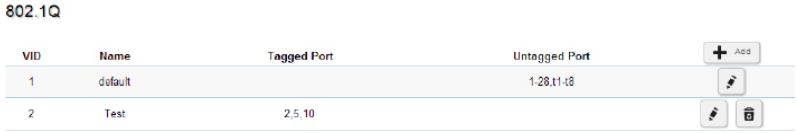


4. Click a radio button in the tagged ports row to select a port.

5. Click the Untagged Ports text box to show the untagged ports dialog box.

6. Click a radio button in the **Untagged Ports** row to select a port.

7. Click **Confirm** to accept the changes or **Cancel** to discard them.



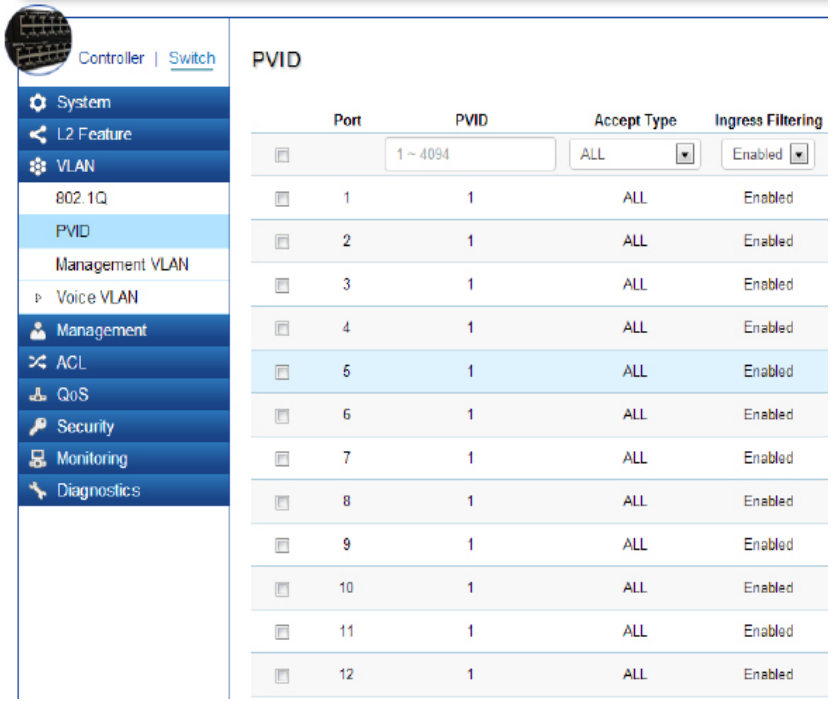
To delete an item in the 802.1Q list, follow these steps:

1. Click the **Delete** button in the row you want to remove an item from. A confirmation dialog will be displayed.

2. Click **OK** to continue or **Cancel** to abort the changes.

PVID

When an Untagged packet enters a Switch port, the PVID (Port VLAN ID) will be attached to the untagged packet and forward frames to a VLAN specified VID part of the PVID. A packet received on a given port would be assigned that port's PVID and then be forwarded to the port that corresponded to the packet's destination address. If the PVID of the port that received the packet is different from the PVID of the port that is to transmit the packet, the Switch will drop the packet. Within the Switch, different PVIDs mean different VLANs, so VLAN identification based upon the PVIDs cannot create VLANs that extend outside a given Switch. If no VLANs are defined on the Switch, all ports are then assigned to a default VLAN with a PVID equal to 1.



Note: To enable PVID functionality, the following requirements must be met:

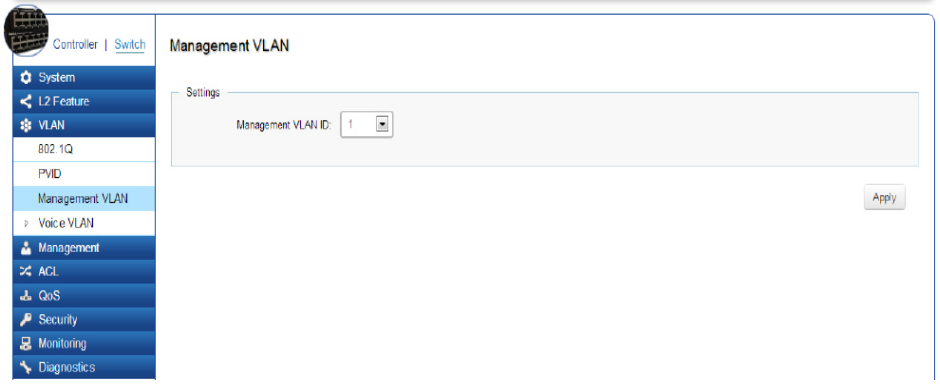
- All ports must have a defined PVID.
- If no other value is specified, the default VLAN PVID is used.
- If you wish to change the port's default PVID, you must first create a VLAN that includes the port as a member.

Port:	Displays the VLAN ID to which the PVID tag is assigned. Configure the PVID to assign untagged or tagged frames received on the selected port.
PVID:	Enter the PVID value. The range is from 1-4094.
Accept Type:	Select **Tagged Only** and **Untagged Only** from the list. • **Tagged Only:** The port discards any untagged frames it's receives. The port only accepts tagged frames. • **Untagged Only:** Only untagged frames received on the port are accepted. • **All**: The port accepts both tagged and untagged frames.
Ingress Filtering:	Specify how you wish the port to handle tagged frames. Select **Enabled** or **Disabled** from the list. • **Enabled:** tagged frames are discarded if VID does not match the PVID of the port. • **Disabled:** All frames are forwarded in accordance with the IEEE 802.1Q VLAN.

Click **APPLY** to update the the system settings.

Management VLAN

The Management VLAN allows users to transfer the authority of the Switch from the default VLAN to other VLAN IDs. By default, the active management VLAN ID is 1, which allows an IP connection to be established through any port. When the management VLAN is set to a different VLAN, connectivity through the existing management VLAN is lost and an IP connection can be made only through a port that is part of the management VLAN. It is also mandatory that the port VLAN ID (PVID) of the port to be connected in that management VLAN be the same as the management VLAN ID.



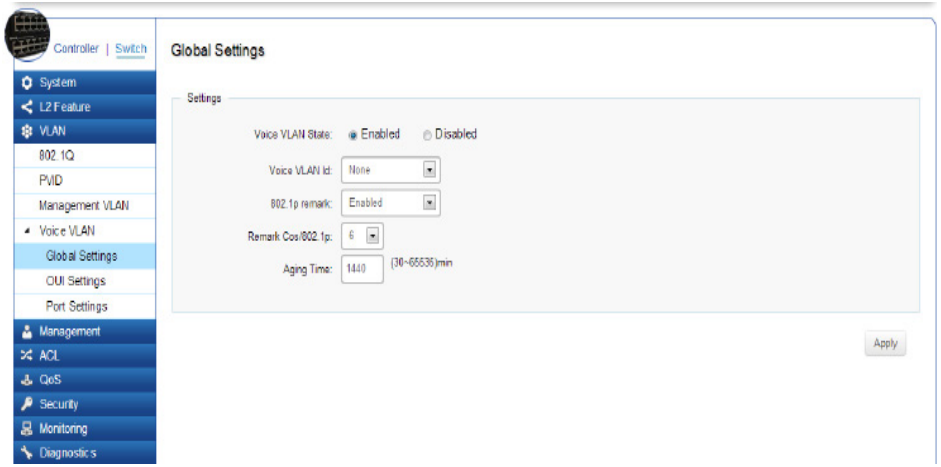
Management VLAN ID:	Select the VLAN ID for allows user to transfer the authority of the Switch.

Apply: Click **Apply** to update the system settings.

Voice VLAN

Enhance your Voice over IP (VoIP) service by configuring ports to carry IP voice traffic from IP phones on a specific VLAN. Voice VLAN provides QoS to VoIP, ensuring that the quality of the call does not deteriorate if the IP traffic is received erratically or unevenly.

Global Settings

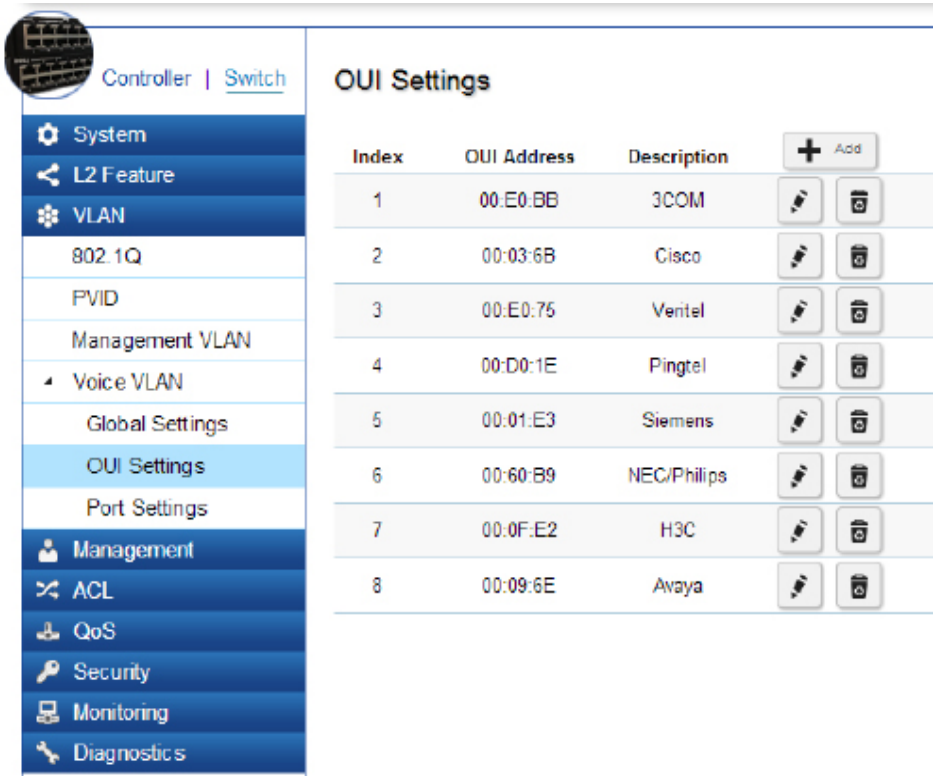


Voice VLAN State:	Select **Enabled** or **Disabled** for Voice VLAN on the Switch.
Voice VLAN ID:	Sets the Voice VLAN ID for the network. Only one Voice VLAN is supported on the Switch.
802.1p Remark:	Enable this function to have outgoing voice traffic to be marked with the selected CoS value.
Remark CoS/802.1p:	Defines a service priority for traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new priority when the Voice VLAN feature is active on a port. (Range: 0-7; Default: 6)
Aging Time:	The aging time is used to remove a port from voice VLAN if the port is an automatic VLAN member. When the last voice device stops sending traffic and the MAC address of this voice device is aged out, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after expiration of the voice VLAN aging timer. If the voice traffic resumes during the aging time, the aging timer will be reset and stop. The range for aging time is from 1 - 65535 minutes. The default is 1440 minutes.

Apply: Click **Apply** to update the system settings.

OUI Settings

The Switches determines whether a received packet is a voice packet by checking its source MAC address. VoIP traffic has a preconfigured Organizationally Unique Identifiers (OUI) prefix in the source MAC address. You can manually add specific manufacturer's MAC addresses and description to the OUI table. All traffic received on the Voice VLAN ports from the specific IP phone with a listed OUI is forwarded on the voice VLAN.



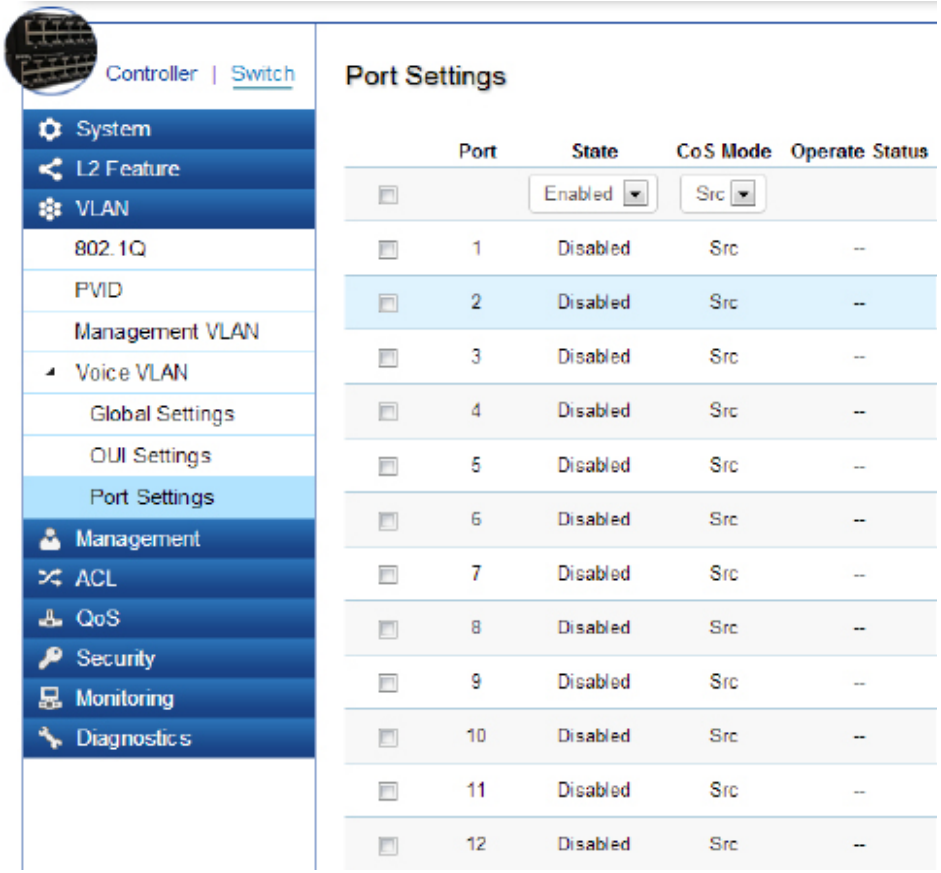
Port:	Enter the OUI to the Voice VLAN. The following OUI are enabled by default. The following OUI are enabled by default. • 00:E0:BB - Assigned to 3COM IP Phones. • 00:03:6B - Assigned to Cisco IP Phones. • 00:E0:75 - Assigned to Veritel IP Phones. • 00:D0:1E - Assigned to Pingtel IP Phones. • 00:01:E3 - Assigned to Siemens IP Phones. • 00:60:B9 - Assigned to NEC/Philips IP Phones. • 00:0F:E2 - Assigned to H3C IP Phones. • 00:09:6E - Assigned to Avaya IP Phones.
Index:	Displays the VoIP sequence ID.
OUI Address:	This is the globally unique ID assigned to a vendor by the IEEE to identify VoIP equipment.
Description:	Displays the ID of the VoIP equipment vendor.

To configure the OUI settings, click the **Edit** button to re-configure the specific entry. Click the **Delete** button to remove the specific entry and click the **Add** button to create a new OUI entry.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Port Settings

Enhance your VoIP service further by configuring ports to carry IP voice traffic from IP phones on a specific VLAN. Voice VLAN provides QoS to VoIP, ensuring that the quality of voice does not deteriorate if the IP traffic is received unevenly.



Port:	Displays the port to which the Voice VLAN settings are applied.
State:	Select **Enabled** to enhance VoIP quality on the selected port. The default is **Disabled**.
CoS Mode:	Select **Src** or **All** from the list.
Src:	Src QoS attributes are applied to packets with OUIs in the source MAC address.
All:	All QoS attributes are applied to packets that are classified to the Voice VLAN.
Operate Status:	Displays the operating status for the Voice VLAN on the selected port.

Apply: Click **Apply** to update the system settings.

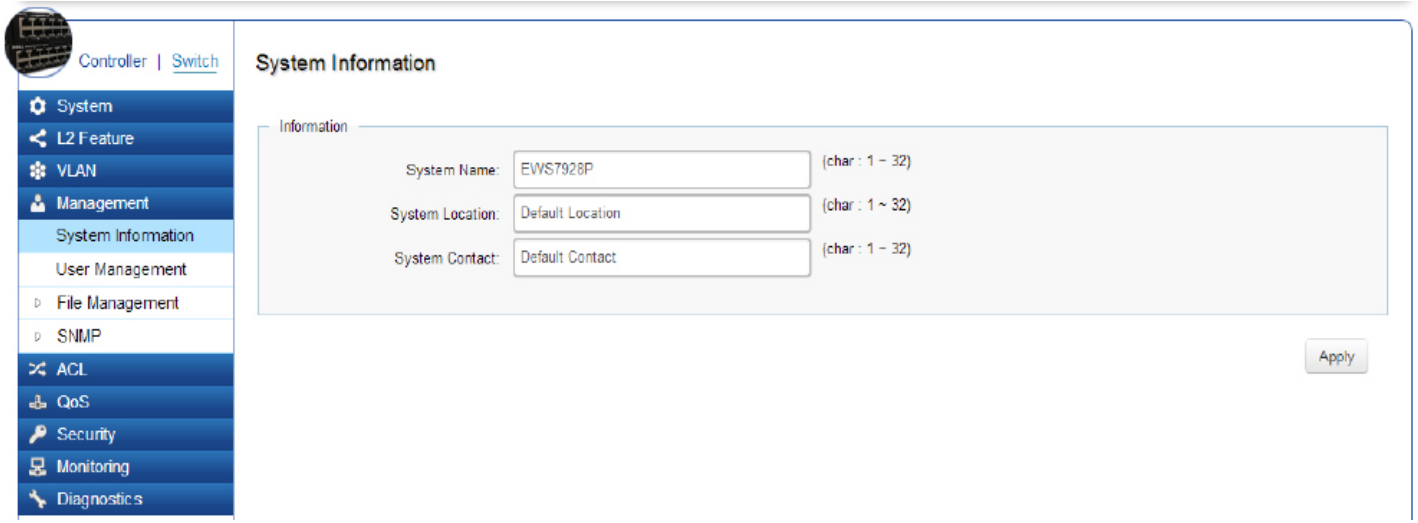
Management

System Information

The System Information screen contains general device information including the system name, system location, and system contact for the Switch.

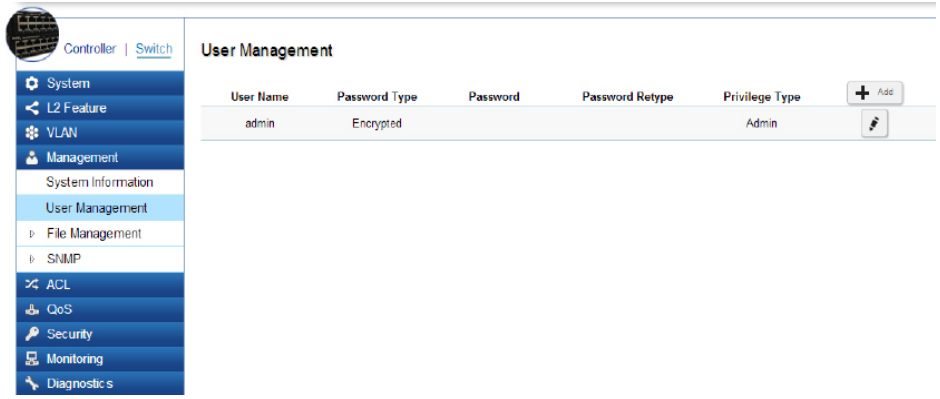
System Name:	Enter the name you wish to use to identify the Switch. You can use up to 32 alphanumeric characters. The factory default name is: **EWS7228P**.
System Location:	Enter the location of the Switch. You can use up to 32 alphanumeric characters. The factory default is: **Default Location**.
System Contact:	Enter the contact person for the Switch. You can use up to 160 alphanumeric characters. The factory default is: **Default Location**.

Click **Apply** to save the changes to the system.



User Management

Use the User Management page to control management access to the Switch based on manually configured user names and passwords. A **User** account can only view settings without the right to configure the Switch, and an **Admin** account can configure all the functions of the Switch. Click the **Add** button to add an account or the **Edit** button to edit an existing account.



User Name:	Enter a username. You can use up to 18 alphanumeric characters.
Password Type:	Select **Clear Text** or **Encrypted** from the list.
Password:	Enter a new password for accessing the Switch.
Password Retype:	Repeat the new password used to access the Switch.
Privilege Type:	Select **Admin** or **User** from the list to regulate access rights.

Important: Note that Admin users have full access rights to the Switch when determining the authority of the user account.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

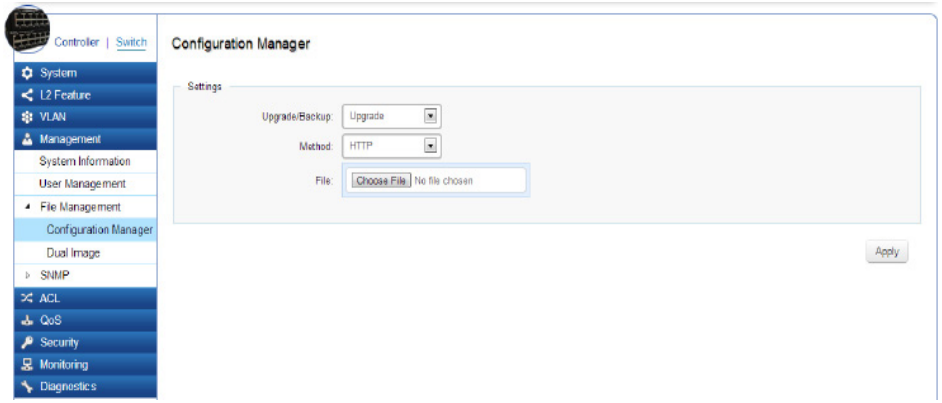
File Management

Configuration Manager

The File Management feature is used for saving your current configuration to a file on your computer or a TFTP server, or to restore previously saved configuration settings to the Switch using a configuration file from your local drive or TFTP server.

Backup

Download the configuration file from the Switch to the TFTP server on the network. Next, download the configuration file from the Switch to your local drive by using an HTTP session.



Upgrade

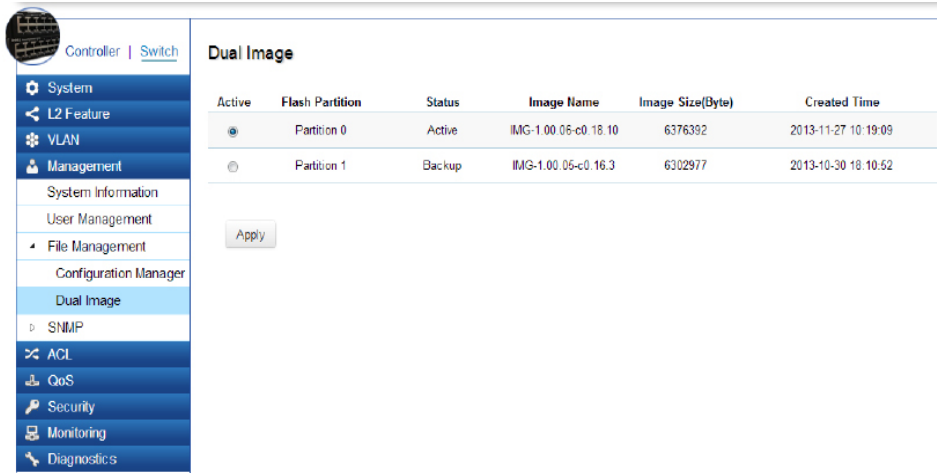
First, upload the configuration file from a TFTP server to the Switch. Next, upload the configuration file from your local drive to the Switch by using an HTTP session.

Upgrade/Backup:	Select **Upgrade** or **Backup** from the list.
Method:	Two methods can be selected; **HTTP** or **TFTP**.
File:	Field only shown when Upgrading via HTTP. Click **Browse** to select file to **Upgrade** or **Backup**.
Server IP:	Enter the Server IP address to upload the configuration file from the TFTP server to the Switch.
File Name:	Field only shown when Upgrading via TFTP. Enter the destination file name of the configuration file to upload from the TFTP server to the Switch.

Click **Apply** to save the changes to the system.

Dual Image

The Switch maintains two versions of the Switch image in its permanent storage. One image is the active image, and the second image is the backup image. The Dual Image screen enables the user to select which partition will be set as active after the next reset. The Switch boots and runs from the active image. If the active image is corrupt, the system automatically boots from the non-active image.



Active:	Selects the partition you wish to be active.
Flash Partition:	Displays the number of the partition.
Status:	Displays the partition which is currently active on the Switch.
Image Name:	Displays the name/version number of the image
Image Size:	Displays the size of the image file.
Created Time:	Displays the time the image was created.

Click **Apply** to save the changes to the system.

SNMP

Simple Network Management Protocol (SNMP) is an Application Layer protocol designed specifically for managing and monitoring network devices. Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from and configuring network devices such as; servers, printers, hubs, Switches, and routers on an Internet Protocol (IP) network. SNMP is used to exchange management information between a network management system (NMS) and a network device. A manager station can manage and monitor the Switch through their network via SNMPv1, v2c and v3. An SNMP managed network consists of two components; agents and a manager.

An agent translates the local management information from the managed Switch into a form that is compatible with SNMP. SNMP allows a manager and agents to communicate with each other for the purpose of accessing Management Information Bases (MIBs). SNMP uses an extensible design, where the available information is defined by MIBs. MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing Object Identifiers (OID). Each OID identifies a variable that can be read or set via SNMP.

The manager is the console through which network administrators perform network management functions.

Several versions of SNMP are supported. They are v1, v2c, and v3. SNMPv1, which is defined in RFC 1157 "A Simple Network Management Protocol (SNMP)", is a standard that defines how communication occurs between SNMP-capable devices and specifies the SNMP message types. Version 1 is the simplest and most basic of versions. There may be times where it's required to support older hardware. SNMPv2c, which is defined in RFC 1901 "Introduction to Community-Based SNMPv2," RFC 1905, "Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)", and RFC 1906 "Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)". SNMPv2c updates protocol operations by introducing a GetBulk request and authentication based on community names. Version 2c adds several enhancements to the protocol, such as support for "Informs". Because of this, v2c has become the most widely used version. Unfortunately, a major weakness of v1 and v2c is security. To combat this, SNMP v3 adds a security features that overcome the weaknesses in v1 and v2c. . If possible, it is recommended that you use v3- especially if you plan to transmit sensitive information across unsecured links. However, the extra security feature makes configuration a little more complex.

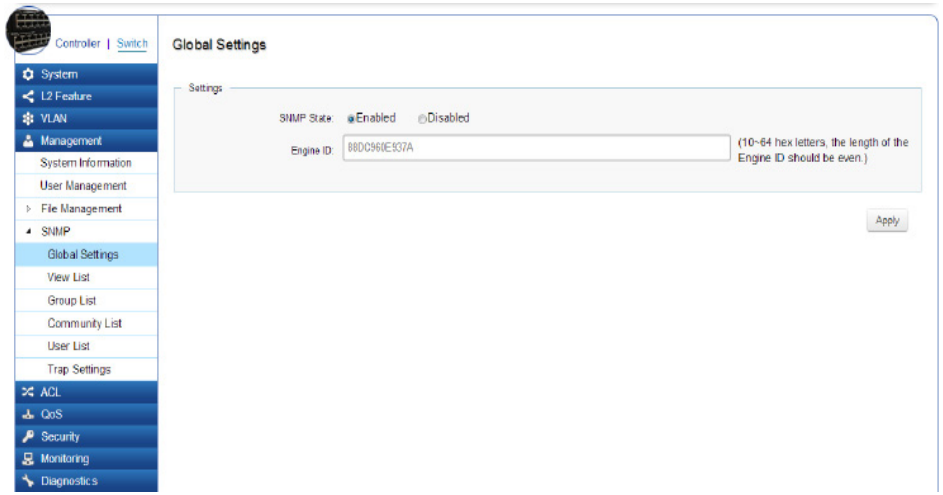
In SNMPv3, User-based Security Model (USM) authentication is implemented along with encryption, allowing you to configure a secure SNMP environment. The SNMPv3 protocol uses different terminology than SNMPv1 and SNMPv2c as well. In the SNMPv1 and SNMPv2c protocols, the terms agent and manager are used. In the SNMPv3 protocol, agents and managers are renamed to entities. With the SNMPv3 protocol, you create users and determine the protocol used for message authentication as well as if data transmitted between two SNMP entities is encrypted.

The SNMPv3 protocol supports two authentication protocols - HMAC-MD5-96 (MD5) and HMAC-SHA-96 (SHA). Both MD5 and SHA use an algorithm to generate a message digest. Each authentication protocol authenticates a user by checking the message digest. In addition, both protocols use keys to perform authentication. The keys for both protocols are generated locally using the Engine ID and the user password to provide even more security.

In SNMPv1 and SNMPv2c, user authentication is accomplished using types of passwords called Community Strings, which are transmitted in clear text and not supported by authentication. Users can assign views to Community Strings that specify which MIB objects can be accessed by a remote SNMP manager.
The default Community Strings for the Switch used for SNMPv1 and SNMPv2c management access for the Switch are public, which allows authorized management stations to retrieve MIB objects, and private, which allow authorized management stations to retrieve and modify MIB objects.

Global Settings

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) protocol designed specifically for managing and monitoring network devices. The SNMP agents maintain a list of variables that are used to manage the device. The variables are defined in the Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent.



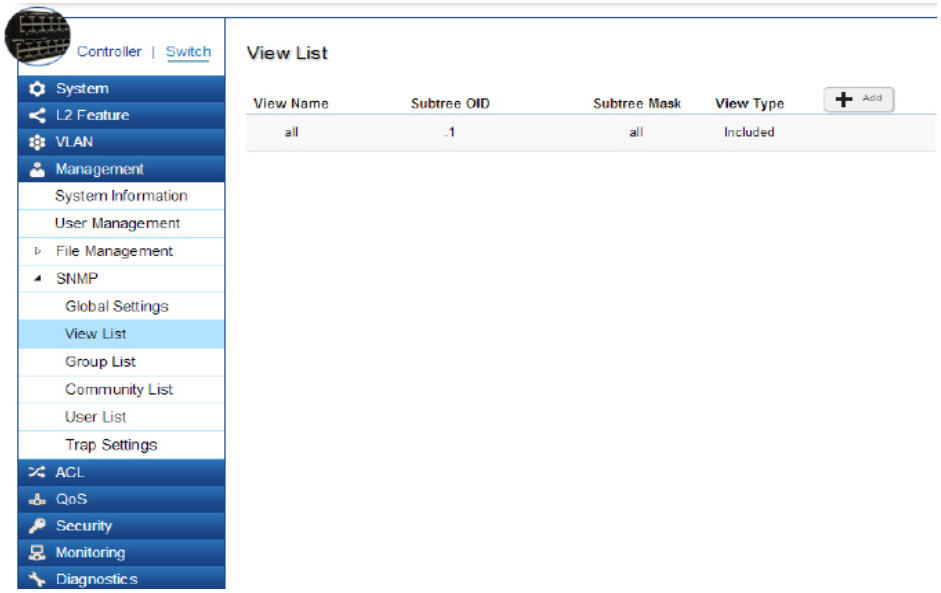
SNMP State:	Enables or Disables the SMNP function. The default SNMP global state is: **Enabled**.
Local Engine ID (10-64 Characters):	Enter the Switch's Engine ID for the remote clients. A SNMPv3 engine is an independent SNMP agent that resides on the Switch. This engine protects against message replay, delay, and redirection issues. The engine ID is also used in combination with user passwords to generate security keys for authenticating and encrypting SNMPv3 packets. Normally, a local engine ID is automatically generated that is unique to the Switch. This is referred to as the default engine ID. If the local engine ID is deleted or changed, all local SNMP users will be cleared and you will need to reconfigure all existing users.

Click **Apply** to save the changes to the system.

View List

SNMP uses an extensible design, where the available information is defined by Management Information bases (MIBs). MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing Object Identifiers (OID) to organize themselves. Each OID identifies a variable that can be read or set via SNMP. The SNMP View List is created for the SNMP management station to manage MIB objects.

Click the **New** button to create a new entry.

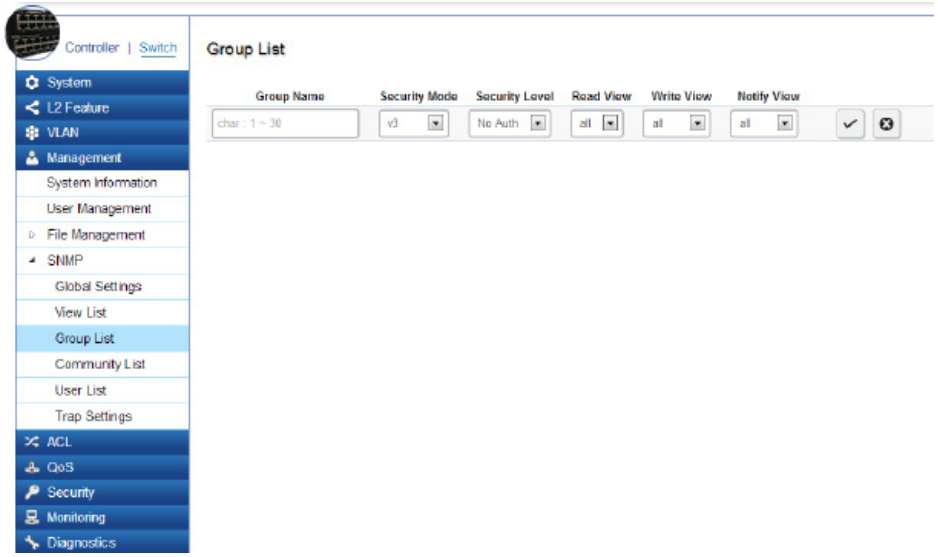


View Name:	Enter the view name. The view name can contain up to 30 alphanumeric characters.
Subtree OID:	Enter the Object Identifier (OID) Subtree. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager. Note that the first character must be a period (.). Wild cards can be used to mask a specific portion of the OID string using a period (.).
Subtree Mask:	Select 0 or 1 for Subtree mask. The mask of the Subtree OID 1 means this object number "is concerned", amd 0 means "do not concern".
View Type:	Select whether the defined OID branch within MIB tree will be included or excluded from the selected SNMP view. Generally, if the view type of an entry is **Excluded**, another entry of view type **Included** should exist and its OID subtree should overlap the **Excluded** view entry.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Group List

Configure SNMP Groups to control network access on the Switch by providing users in various groups with different management rights via the Read View, Write View, and Notify View options.



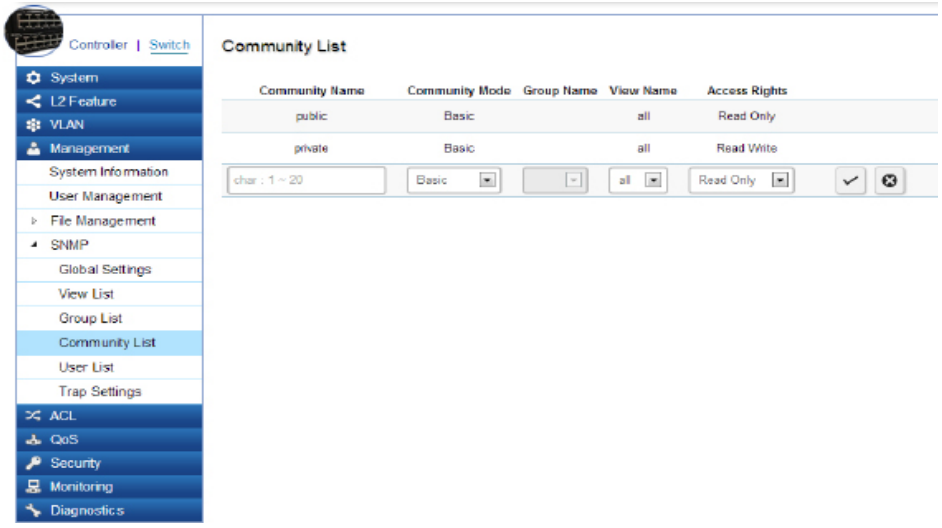
Group Name:	Enter the group name that access control rules are applied to. The group name can contain up to 30 alphanumeric characters.
Security Mode:	Selects the SNMP version (v1, v2c, v3) associated with the group.
Security Level:	Select the security level for the group. Security levels apply to SNMPv3 only. • **No Auth** - Neither authentication nor the privacy security levels are assigned to the group. • **Auth** - Authenticates SNMP messages. • **Priv** - Encrypts SNMP messages.
Read View:	Management access is restricted to read-on-only.
Write View:	Select a SNMP to allow SNMP write privileges to the Switch's SNMP agent.
Notify View:	Select a SNMP group to receive SNMP trap messages generated by the Switch's SNMP agent.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Community List

In SNMPv1 and SNMPv2c, user authentication is accomplished using types of passwords called Community Strings, which are transmitted in clear text and not supported by authentication. It is important to note that the community name can limit access to the SNMP agent from the SNMP network management station, functioning as a password.

Click **Add** to add a community list to the Switch. Next, name the community and choose the level of access that will be granted to the specified list from the drop-down boxes.

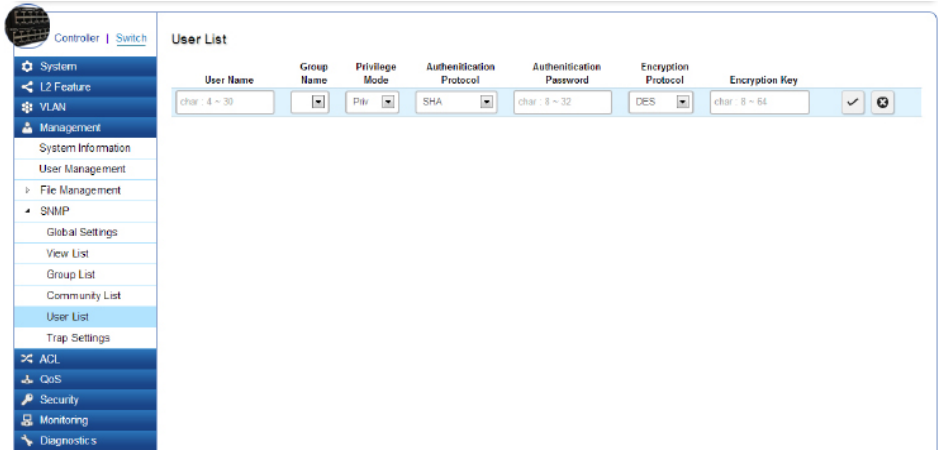


Community Name:	Enter the name of SNMP community string.
Community Mode:	Selected **Basic** or **Advance** from the list. Select the Advance attached to the SNMP group.
Group Name:	Select the SNMP group from a list.
View Name:	Select the view name from a list.
Access Rights:	Specify the level of permission for the MIB objects accessible to the SNMP. Your choices are **Read/write** or **Read-only**.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

User List

Use the User List page to create SNMP users for authentication with managers using SNMP v3 to associate them to SNMP groups. Click **Add** to add a new user.



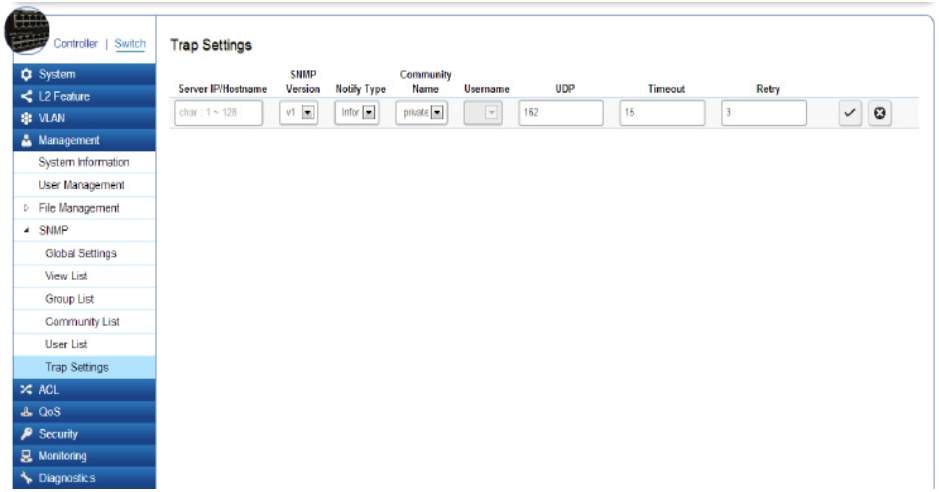
Privilege Mode:	Select **No Auth**, **Auth**, or **Priv** security level from the list. • **No auth -** Neither authentication nor the privacy security levels are assigned to the group. • **Auth -** and ensures that the origin of the SNMP message is authenticated. • **Priv -** Encrypts SNMP messages.
Authentication Protocol:	Select the method used to authenticate users. • **MD5 -** Using the HMAC-MD5 algorithm. • **SHA -** Using the HMAC-SHA-96 authentication level. Enter the SHA password and the HMAC-SHA-96 password to be used for authentication.
Authentication Password:	Enter MD5 password and the HMAC-MD5-96 password to be used for authentication.
Encryption Protocol:	Select the method used to authenticate users. • **None -** No user authentication is used. • **DES -**Using the Data Encryption Standard algorithm.
Encryption Key:	Enter the Data Encryption Standard key.

Click the **Apply** button to accept the changes or the

Trap Settings

SNMP Traps

A trap is a type of SNMP message. The Switch can send traps to an SNMP manager when an event occurs.
You can restrict user privileges by specifying which por¬tions of the MIBs that a user can view. In this way, you restrict which MIBs a user can display and modify for better security. In addition, you can restrict the types of traps users can send as well. You can do this by determining where messages are sent and what types of messages can be sent per user. Traps indicating status changes can be issued by the Switch to the specified trap manager by sending authentication failure messages and other trap messages.



ACL

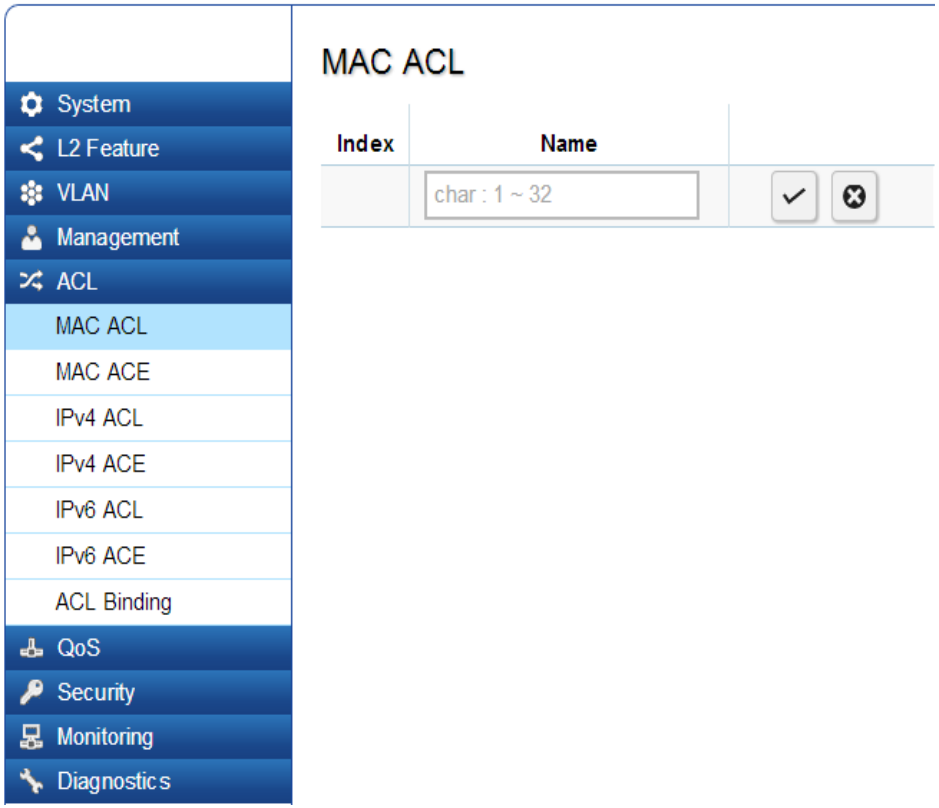
An Access Control List (ACL) allows you to define classifi¬cation rules or establish criteria to provide security to your network by blocking unauthorized users and allowing authorized us¬ers to access specific areas or resources. ACLs can provide basic security for access to the network by controling whether packets are forwarded or blocked at the Switch ports. Access Control Lists (ACLs) are filters that allow you to classify data packets according to a particular content in the packet header, such as the source address, destination address, source port number, destination port number, and more. Packet classifiers identify flows for more efficient processing. Each filter defines the conditions that must match for inclusion in the filter. ACLs (Access Control Lists) provide packet filtering for IP frames (based on the protocol, TCP/UDP port number or frame type) or layer 2 frames (based on any destination MAC address for unicast, broadcast, or multicast, or based on VLAN ID or VLAN tag priority). ACLs can be used to improve performance by blocking unnecessary network traffic or to implement security controls by restricting access to specific network resources or protocols. Policies can be used to differentiate service for client ports, server ports, network ports, or guest ports. They can also be used to strictly control network traffic by only allowing incoming frames that match the source MAC and source IP address on a specific port. ACLs are composed of Access Control Entries (ACEs), which are rules that determine traffic classifications. Each ACE is a considered as a single rule, and up to 256 rules may be defined on each ACL, with up to 3000 rules globally. ACLs are used to provide traffic flow control, restrict contents of routing updates, and determine which types of traffic are forwarded or blocked. This criterion can be specified on a basis of the MAC address or IP address.

Server IP/Hostname:	Enter the Server IP or Hostname. The Hostname can contain up to 128 alpha-numeric characters.
SNMP Version:	Select the SNMP version from the list.
Notify Type:	Select the type of notification to be sent. • **Traps –** Traps are sent. • **Informs –** Informs are sent **ONLY** when v2c is enabled. **Note:** The recipient of a trap message does not send a response to the Switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Inform messages can be used to ensure that critical information is received by the host. However, please note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.
Community Name:	Select the Community Name from the list.
UDP:	Enter the UDP port used to send notifications.
Timeout:	Configurable only if the notify type is I**nforms**. Enter the amount of time the device waits before re-sending. The default is 15 seconds.
Retry:	Configurable only if the notify type is **Informs**. Enter the amount of time the device waits before re-sending an inform request. The default is 3 seconds.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

MAC ACL

This page displays the currently-defined MAC-based ACLs profiles. To add a new ACL, click **Add** and enter the name of the new ACL.

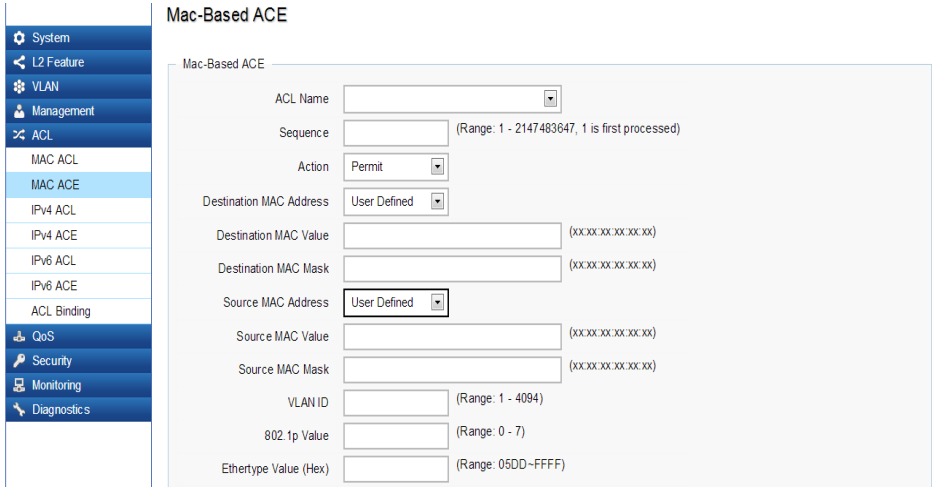


Index:	Profile identifier.
Name:	Enter the MAC based ACL name. You can use up to 32 alphanumeric characters.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Mac-Based ACE

Use this page to view and add rules to MAC-based ACLs.

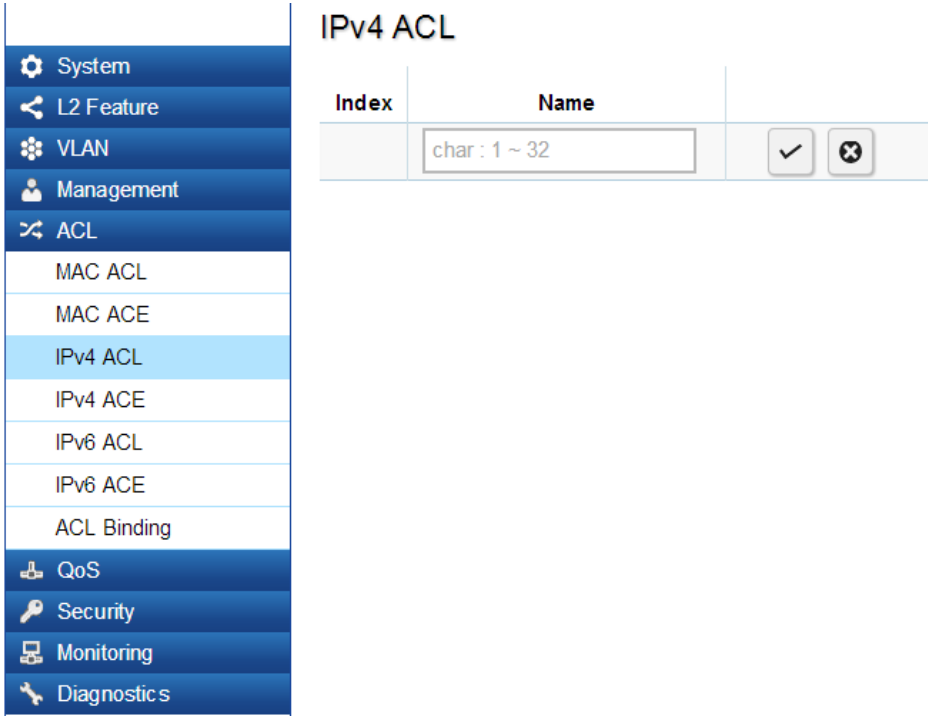


ACL Name:	Select the ACL from the list.
Sequence:	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected interface. The valid range is from 1-2147483646, 1 being processed first.
Action:	Select what action taken if a packet matches the criteria. • **Permit** - Forward packets that meet the ACL criteria. • **Deny**- Drops packets that meet the ACL criteria.

Destination MAC Value:	Enter the destination MAC address.
Destination MAC Wildcard Mask:	Enter a MAC address mask for the destination MAC address. A mask of 00:00:00:00:00:00 means the bits must be matched exactly; ff:ff:ff:ff:ff:ff means the bits are irrelevant. Any combination of 0s and ffs can be used.
Source MAC Value:	Enter the source MAC address.
Source MAC Wildcard Mask:	Enter a MAC address mask for the source MAC address. A mask of 00:00:00:00:00:00 means the bits must be matched exactly; ff:ff:ff:ff:ff:ff means the bits are irrelevant. Any combination of 0s and ffs can be used.
VLAN ID:	Enter the VLAN ID to which the MAC address is attached in MAC ACE. The range is from 1-4094.
802.1p Value:	Enter the 802.1p value. The range is from 0-7.
Ethertype Value:	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header. This option can only be used to filter Ethernet II formatted packets. A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), and 8137 (IPX).

IPv4 ACL

This page displays the currently-defined IPv4-based ACLs profiles. To add a new ACL, click **Add** and enter the name of the new ACL.

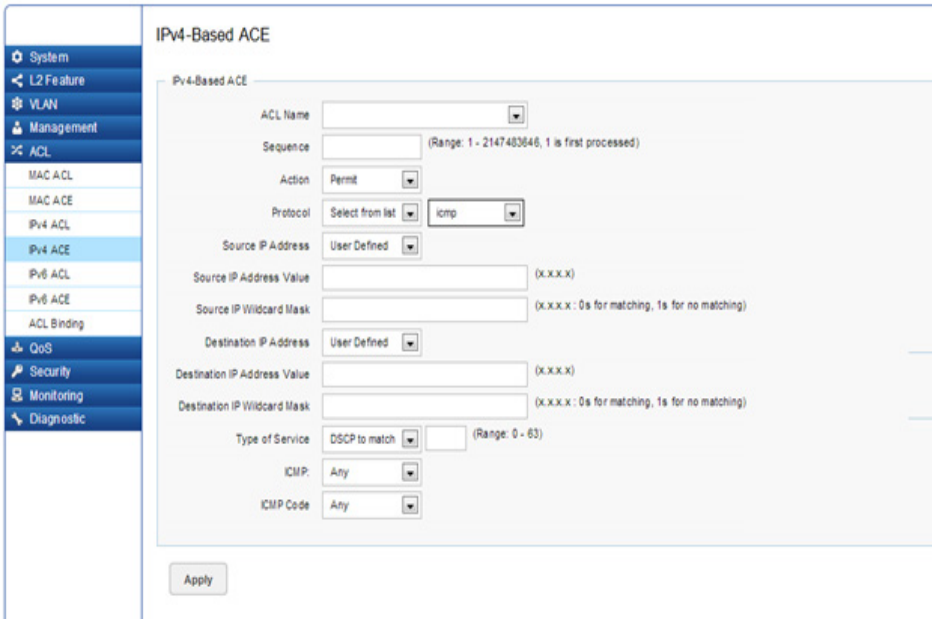


Index:	Displays the current number of ACLs.
Name:	Enter the IP based ACL name. You can use up to 32 alphanumeric characters.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

IPv4-Based ACE

Use this page to view and add rules to IPv4-based ACLs.



ACL Name:	Select the ACL from the list for which a rule is being created.
Sequence:	Enter the priority of the ACE. ACEs with a higher priority are processed first. 1 is the highest priority.

Action:	Select what action to take if a packet matches the criteria. • **Permit** - Forwards packets that meet the ACL criteria. • **Deny**- Drops packets that meet the ACL criteria.
Protocol:	Select **Any**, **Protocol ID,** or **Select from a List** in the drop down menu. • **Any -** Check Any to use any protocol. • **Protocol ID** - Enter the protocol in the ACE to which the packet is matched. • **Select from List**-Selects the protocol from the list in the provided field. • **ICMP** – Internet Control Message Protocol (ICMP). The ICMP enables the gateway or destination host to communicate with the source host. • **IPinIP** – IP in IP. Encapsulates IP packets to create tunnels between two routers. This ensures that IPIP tunnel appears as a single interface, rather than several separate interfaces. IPIP enables tunnel intranets occur the internet, and provides an alternative to source routing. • **TCP** – Transmission Control Protocol (TCP). Enables two hosts to communicate and exchange data streams. TCP guarantees packet delivery, and guarantees that packets are transmitted and received in the order they are sent.

	• **EGP** – Exterior Gateway Protocol (EGP). Permits exchanging routing information between two neighboring gateway hosts in an autonomous systems network. • **IGP** – Interior Gateway Protocol (IGP). Enables a routing information exchange between gateways within an autonomous network. • **UDP** – User Datagram Protocol (UDP). UDP is a communication protocol that transmits packets but does not guarantee their delivery. • **HMP** – The Host Mapping Protocol (HMP) collects network information from various networks hosts. HMP monitors hosts spread over the internet as well as hosts in a single network. • **RDP** – Reliable Data Protocol (RDP). provides a reliable data transport service for packet-based applications. • **IPv6** - Matches the packet to the IPV6 protocol. • **IPv6**: Rout -Routing Header for IPv6. • **IPv6**: Frag -Fragment Header for IPv6. • **RVSP** – Matches the packet to the ReSerVation Protocol(RSVP). •**IPv6**: ICMP - The Internet Control Message Protocol (ICMP) allows the gateway or destination host to communicate with the source host.

	• OSPF – The Open Shortest Path First (OSPF) protocol is a link-state hierarchical interior gateway protocol (IGP) for network routing Layer Two (2) Tunneling Protocols. It is an an extension to the PPP protocol that enables ISPs to operate Virtual Private Networks (VPNs). • PIM – Matches the packet to Protocol Independent Multicast (PIM). • L2TP – Matches the packet to Internet Protocol (L2IP).
Destination IP Address Value:	Enter the destination IP address.
Destination IP Wildcard Mask:	Enter the mask of the new source IP address.
Source IP Address Value:	Enter the source IP address.

Click **Apply** to save the changes to the system.

IPv6 ACL

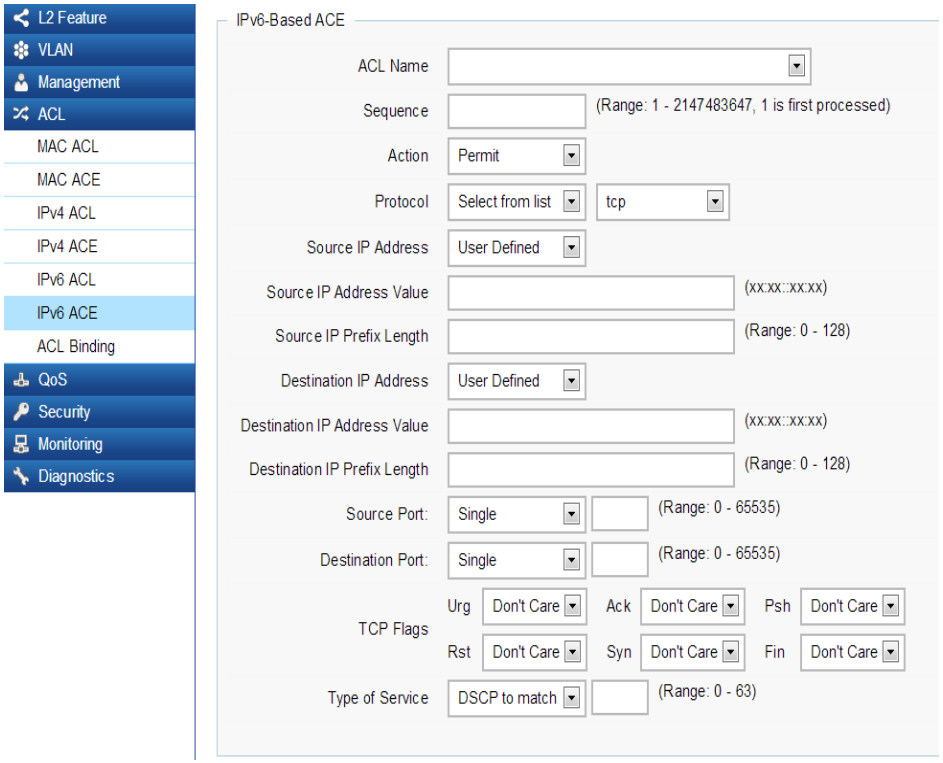
This page displays the currently-defined IPv6-based ACLs profiles. To add a new ACL, click **Add** and enter the name of the new ACL.

Index:	Displays the current number of ACLs.
Name:	Enter the IPv6 based ACL name. You can use up to 32 alphanumeric characters.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

IPv6 Based ACE

Allows IPv6 Based Access Control Entry (ACE) to be defined within a configured ACL.



ACL Name:	Select the ACL from the list.
Sequence:	Enter the sequence number which signifies the order of the specified ACL relative to other ACLs assigned to the selected interface. The valid range is from 1-2147483646, 1 being processed first.
Action:	Select what action taken if a packet matches the criteria. • **Permit** – Forward packets that meet the ACL criteria. • **Deny**– Drops packets that meet the ACL criteria.
Protocol:	Select the **Any**, **Protocol ID**, or **Select from List** from drop down menu. • **Protocol ID** – Enter the protocol in the ACE to which the packet is matched. • **Select from List**–Select the protocol from the list in the provided field.
Destination IP Address Value:	Enter the destination IP address.
Destination IP Wildcard Mask:	Enter the mask of the new source IP address.
Source IP Address Value:	Enter the source IP address.
Source IP Wildcard Mask:	Enter the mask of the new source IP address.

VLAN ID:	Enter the VLAN ID to which the IP address is attached in IPv4-Based ACE. The range is from 1-4094.
802.1p Value:	Enter the 802.1p value. The range is from from 0-7.
Ethertype Value:	Enter the Ethertype value. The range is from 05DD-FFFF.
ICMP:	Select **Any**, **Protocol ID**, or **Select from List** from drop down menu. • **Protocol ID** – Enter the protocol in the ACE to which the packet is matched. The range is from 0-255. • **Select from List**– Select the ICMP from the list in the provided field.
ICMP Code:	Enter the ICMP code. The range is from 0-255.
Source Port:	Select **Single** or **Range** from the list. Enter the source port that is matched to packets. The range is from 0-65535.
Destination Port:	Select **Single** or **Range** from the list. Enter the destination port that is matched to packets. The range is from 0-65535.
Type of Service:	Enter the DSCP. The range is from 0-63.

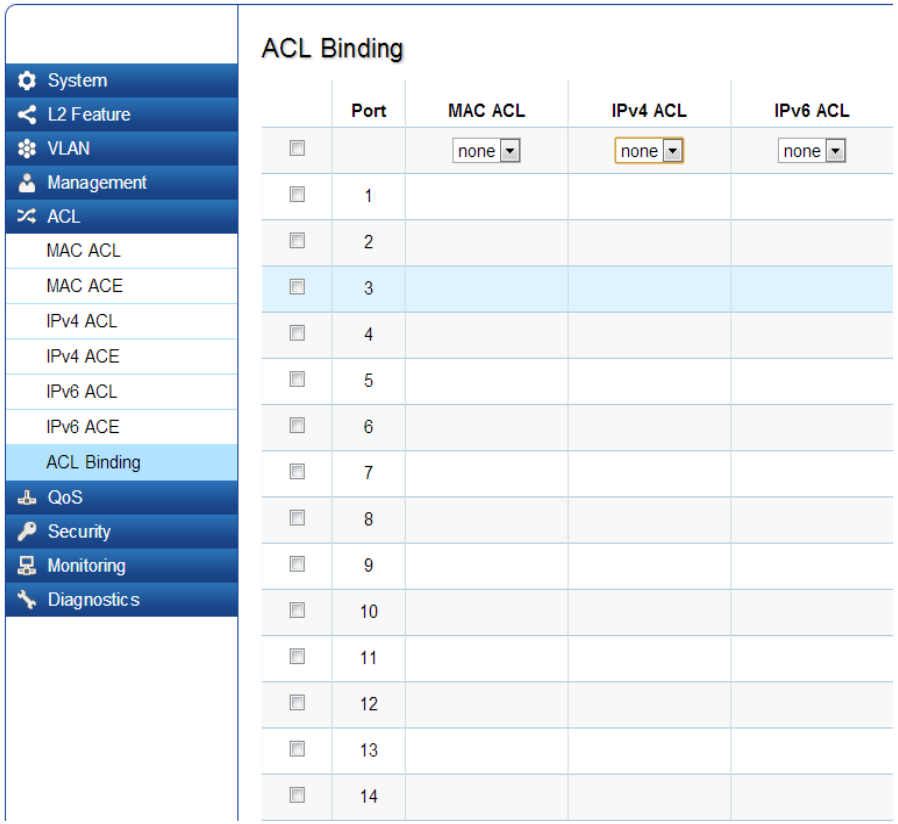
Click **Apply** to save the changes to the system.

ACL Binding

When an ACL is bound to an interface, all the rules that have been defined for the ACL are applied to that interface. Whenever an ACL is assigned on a port or LAG, flows from that ingress or egress interface that do not match the ACL, are matched to the default rule of dropping unmatched packets. To bind an ACL to an interface, simply select an interface and select the ACL(s) you wish to bind.

Port:	Select the port for which the ACLs are bound to.
MAC ACL:	The ACL is MAC address based.
IPv4 ACL:	The ACL is IP address based.
IPv6 ACL:	The ACL is IP address based.

Click **Apply** to save the changes to the system.



QoS

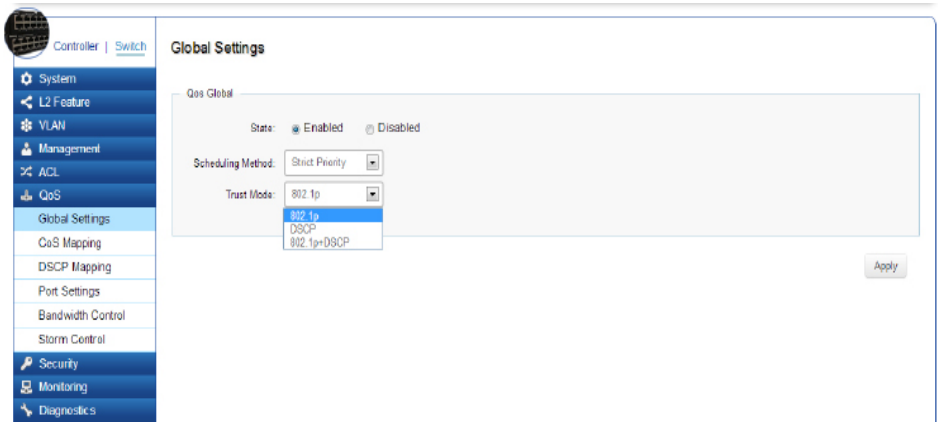
Quality of Service (QoS) provides the ability to implement priority queuing within a network. QoS is a means of providing consistent and predictable data delivery to the Switch by distinguishing between packets that have stricter timing requirements from those that are more tolerant of delays. QoS enables traffic to be prioritized while avoiding excessive broadcast and multicast traffic. Traffic such as Voice and Video streaming which require minimal delays can be assigned to a high priority queue, while other traffic can be assigned to a lower priority queue, resulting in uninterrupted actions. Without QoS, all traffic data is as likely to be dropped when the network is congested. This can result in reductions in network performance and hinder the network in time-critical situations.

In a Switch, multiple queues per port are often provided to give preference to certain packets over others based on user-defined criteria. When a packet is queued for transmission within a port, the rate at which it is processed depends on how the queue is configured and the amount of traffic present within other queues on the port. If a delay is necessary, packets are held in the queue until they are authorized for transmission.

Global Settings

There are two options for applying QoS information onto packets: the 802.1p Class of Service (CoS) priority field within the VLAN tag of tagged Ethernet frames, and Differentiated Services (DiffServ) Code Point (DSCP). Each port on the Switch can be configured to trust one of the packet fields (802.1p , DSCP or DSCP+802.1p). Packets that enter the Switch's port may carry no QoS information as well. If so, the Switch places such information into the packets before transmitting them to the next node. Thus, QoS information is preserved between nodes within the network and the nodes know which label to give each packet. A trusted field must exist in the packet for the mapping table to be of any use. When a port is configured as untrusted, it does not trust any incoming packet priority designations and uses the port default priority value instead to process the packet.

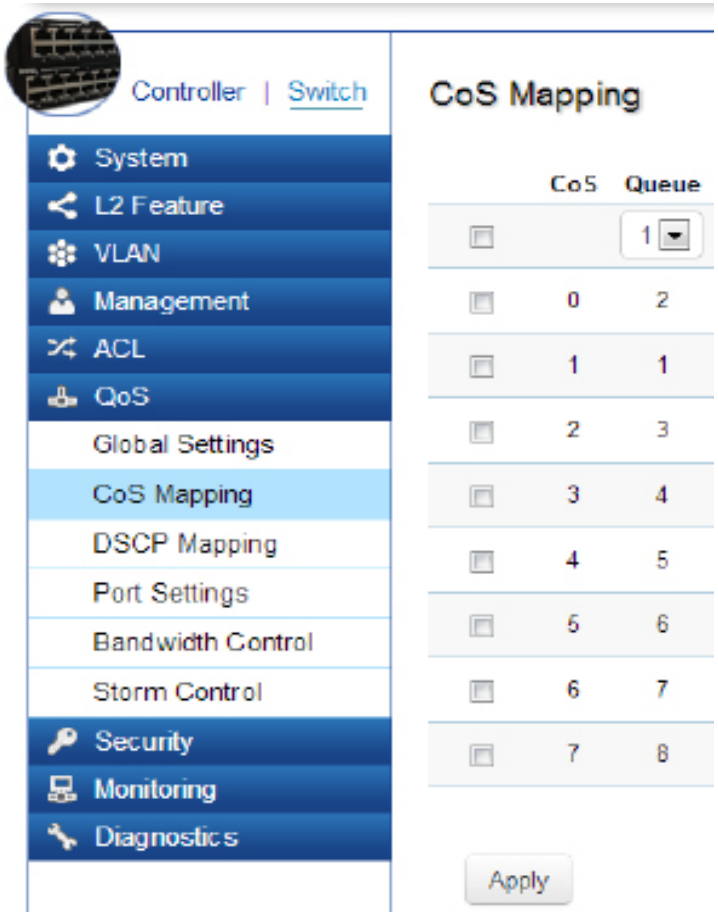
State:	Select whether QoS is enabled or disabled on the switch.
Scheduling Method:	Selects the Strict Priority or WRR to specify the traffic scheduling method. • **Strict Priority -** Specifies traffic scheduling based strictly on the queue priority. • **WRR -** Use the Weighted Round-Robin (WRR) algorithm to handle packets in priority classes of service. It assigns WRR weights to queues.
Trust Mode:	Select which packet fields to use for classifying packets entering the Switch. • **DSCP** - Classify traffic based on the DSCP (Differentiated Services Code Point) tag value. • **1p**-Classify traffic based on the 802.1p. The eight priority tags that are specified in IEEE802.qp are from 1 to 8.



Click **Apply** to save the changes to the system.

CoS Mapping

Use the Class of Service (CoS) Mapping feature to specify which internal traffic class to map to the corresponding CoS value. CoS allows you to specify which data packets have greater precedence when traffic is buffered due to congestion.

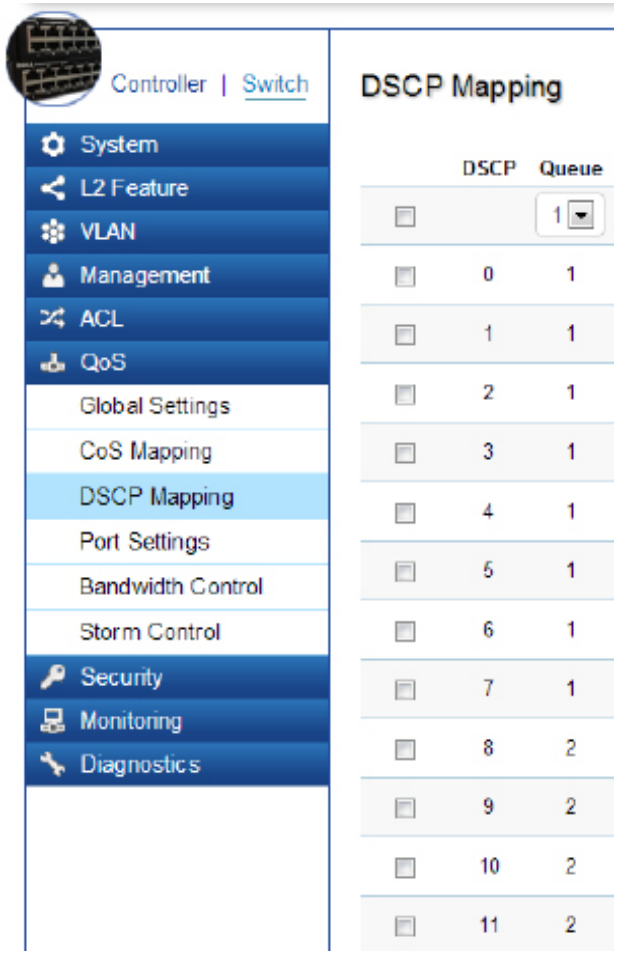


CoS (Class of Service):	Displays the CoS priority tag values, where 0 is the lowest and 7 is the highest.
Queue:	Check the CoS priority tag box and select the Queue values for each CoS value in the provided fields. Eight traffic priority queues are supported and the field values are from 1-8, where one is the lowest priority and eight is the highest priority.

Click **Apply** to save the changes to the system.

DSCP Mapping

Use Differentiated Services Code Point (DSCP) Mapping feature to specify which internal traffic class to map to the corresponding DSCP values. DSCP Mapping increases the number of definable priority levels by reallocating bits of an IP packet for prioritization purposes.



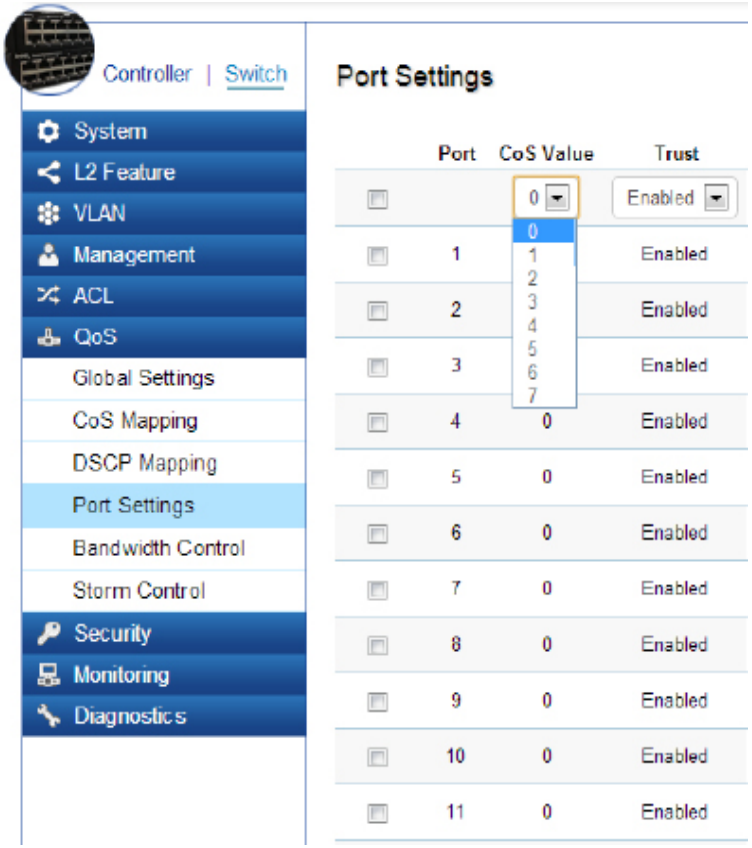
DSCP (Differentiated Services Code Point):	Displays the packet's DSCPvalues, where 0 is the lowest and 10 is the highest.
Queue:	Check the CoS priority tag box and select the Queue values for each DSCP in the provided fields. Eight traffic priority queues are supported and the field values are from 1-8, where one is the lowest priority and eight is the highest priority.

Click **Apply** to save the changes to the system.

Port Settings

From here, you can configure the QoS port settings for the Switch. Select a port you wish to set and choose a CoS value from the drop-down box. Next, Select to **Enable** or **Disable** the Trust setting to let any CoS packet be marked at ingress.

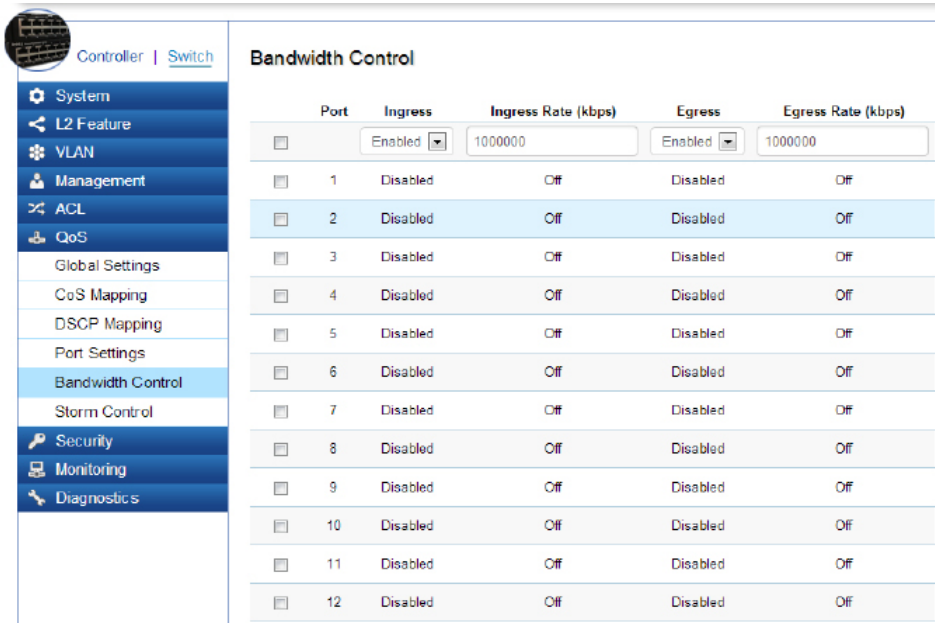
Port:	Displays the ports for which the CoS parameters are defined.
CoS (Class of Service) Value:	Select the CoS priority tag values, where 0 is the lowest and 7 is the highest.
Trust:	Select **Enable** to trust any CoS packet marking at ingress and select **Disable** to not trust any CoS packet marking at ingress.



Click **Apply** to save the changes to the system.

Bandwidth Control

The Bandwidth Control feature allows users to define the bandwidth settings for a specified port's Ingress Rate Limit and Egress Rate.

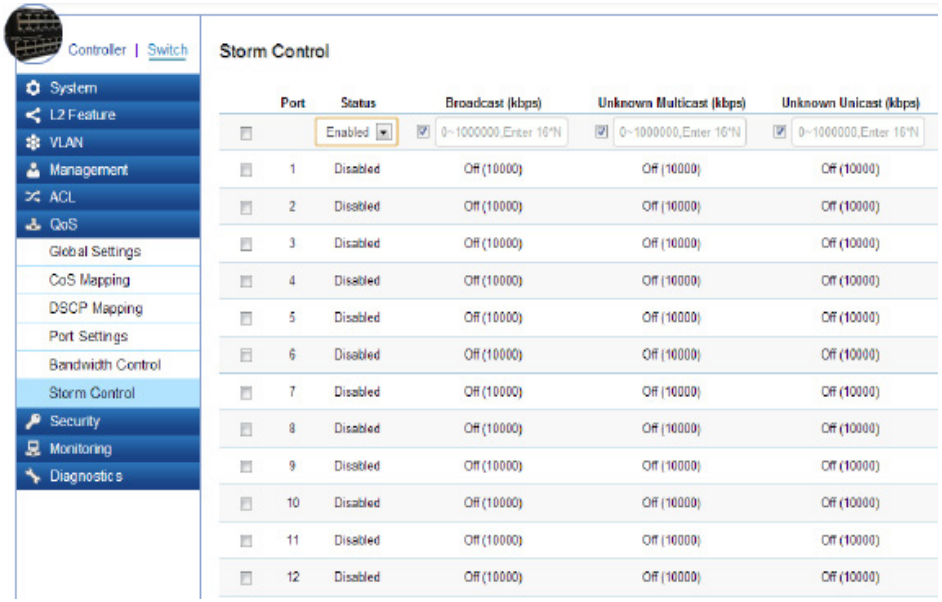


Port:	Displays the ports for which the bandwidth settings are displayed.
Ingress:	Select to **Enable** or **Disable** ingress on the interface.
Ingress Rate:	Enter the ingress rate in kilobits per second. The Gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second.
Egress:	Select from the drop down box to **Enable** or **Disable** egress on the interface .
Egress Rate:	Enter the egress rate in kilobits per second. The Gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second.

Click **Apply** to save the changes to the system.

Storm Control

Storm Control limits the amount of Broadcast, Unknown Multicast, and Unknown Unicast frames accepted and forwarded by the Switch. Storm Control can be enabled per port by defining the packet type and the rate that the packets are transmitted at. The Switch measures the incoming Broadcast, Unknown Multicast, and Unknown Unicast frames rates separately on each port, and discards the frames when the rate exceeds a user-defined rate.



Port:	Displays the ports for which the Storm Control information is displayed.
Status:	Select whether Storm Control is **Enabled** or **Disabled** ingress on the interface.
Broadcast:	Enter the **broadcast** rate in kilobits per second. The Gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second. If the rate of broadcast traffic ingress on the interface increases beyond the configured threshold, the traffic is dropped.
Unknown Multicast:	Enter the Unknown Multicast rate in kilobits per second. The Gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second. If the rate of broadcast traffic ingress on the interface increases beyond the configured threshold, the traffic is dropped.
Unknown Unicast:	Enter the Unknown Unicast rate in kilobits per second. The Gigabit Ethernet ports have a maximum speed of 1000000 kilobits per second. If the rate of broadcast traffic ingress on the interface increases beyond the configured threshold, the traffic is dropped.

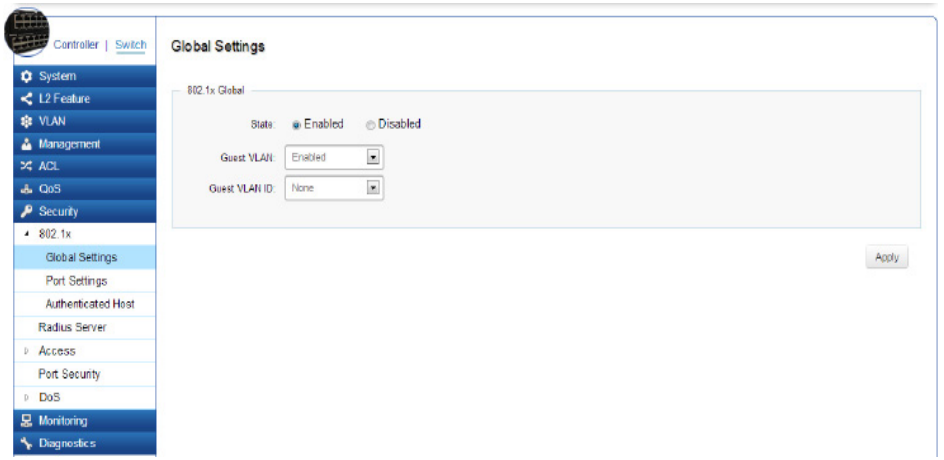
Security

802.1X

The IEEE 802.1X standard authentication uses the RADIUS (Remote Authentication Dial In User Service) protocol to validate users and provide a security standard for network access control. The user that wishes to be authenticated is called a supplicant. The actual server doing the authentication, typically a Radius server, is called the authentication server. The mediating device, such as a Switch, is called the authenticator. Clients connected to a port on the Switch must be authenticated by the Authentication Server (Radius) before accessing any services offered by the Switch on the LAN. Use a Radius server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the Client and Server. This establishes the requirements needed for a protocol between the authenticator (the system that passes an authentication request to the authentication server) and the supplicant (the system that requests authentication), as well as between the authenticator and the authentication server.

Global Settings

When a supplicant is connected to a Switch port, the port issues an 802.1X authentication request to the attached the 802.1X supplicant. The supplicant replies with the given username and password and an authentication request is then passed to a configured Radius server. The authentication server's user database supports Extended Authentication Protocol (EAP), which allows particular guest VLAN memberships to be defined based on each individual user. After authorization, the port connected to the authenticated supplicant then becomes a member of the specified guest VLAN. When the supplicant is successfully authenticated, traffic is automatically assigned to the guest VLAN.



Click **Apply** to save the changes to the system.

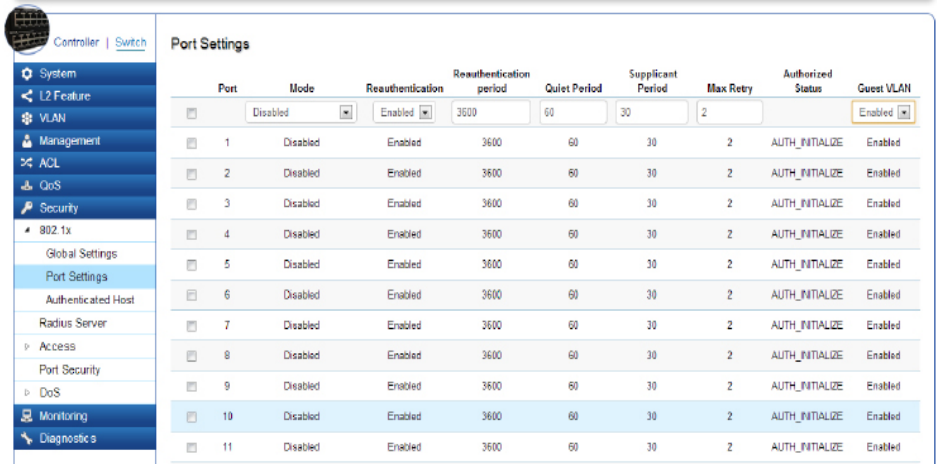
State:	Select whether authentication is **Enabled** or **Disabled** on the Switch.
Guest VLAN:	Select whether Guest VLAN is **Enabled** or **Disabled** on the Switch. The default is **Disabled**.
Guest VLAN ID:	Select the guest VLAN ID from the list of currently defined VLANs.

Port Settings

The IEEE-802.1X port-based authentication provides a security standard for network access control with Radius servers and holds a network port disconnected until authentication is completed. With 802.1X port-based authentication, the supplicant provides the required credentials, such as user name, password, or digital certificate to the authenticator, and the authenticator forwards the credentials to the authentication server for verification to the guest VLAN. If the authentication server determines the credentials are valid, the supplicant is allowed to access resources located on the protected side of the network.

From here, you can configure the port settings as they relate to 802.1X. First, select the mode from the you wish to utilize from the drop-down box. Next, choose whether to **Enable** or **Disable** reauthentification for the port. Enter the time span that you wish to elapse for the Re-authentification period, Quiet Period, and Supplicant Period. After this, enter the max number of times you wish for the Switch to retransmit the EAP request. Finally, choose whether you wish to **Enable** or **Disable** the VLAN ID.

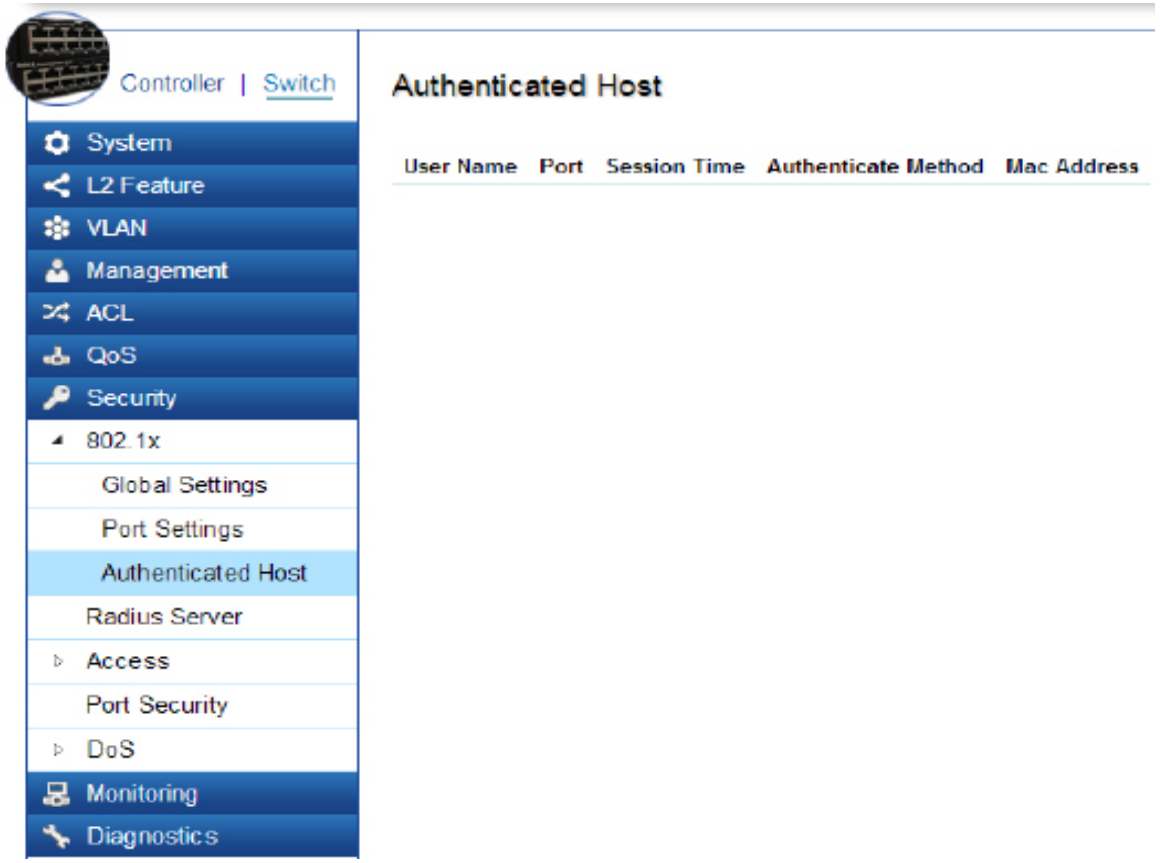
Port:	Displays the ports for which the 802.1X information is displayed.
Mode:	Select the **Auto** or **Force_UnAuthorized** or **Force_Authorized** mode from the list.
Re-Authentication:	Select whether port reauthenticati-on is **Enabled** or **Disabled**.
Re-authentication period:	Enter the time span in which the selected port is reauthenticated. The default is 3600 seconds.
Quiet Period:	Enter the number of the device that remains in the quiet state following a failed authentication exchange. The default is 60 seconds.
Supplicant Period:	Enter the amount of time that lapses before an EAP request is resent to the supplicant. The default is 30 seconds.
Max Retry:	Enter the maximum number of times that the Switch retransmits an EAP request to the client before it times out the authentication session. The default is 2 times.
Guest VLAN ID:	Select whether guest VLAN ID is **Enabled** or **Disabled**.



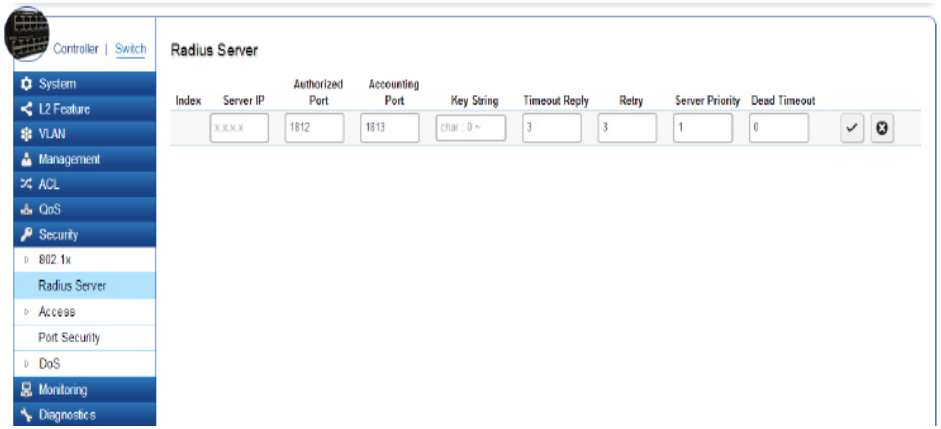
Apply: Click **Apply** to update the system settings.

Authenticated Host

The Authenticated Host section displays the Authenticated User Name, Port, Session Time, Authenticated Method, and Mac Address.



Radius Server



Radius proxy servers are used for centralized administration. Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users that connect and use a network service for greater convenience. Radius is a server protocol that runs in the application layer, using UDP as transport. The Network Switch with port-based authentication and all have a Radius client component that communicates with the Radius server. Clients connected to a port on the Switch must be authenticated by the Authentication Server before accessing services offered by the Switch on the LAN. Use a Radius server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the Client and Server. The Radius server maintains a user database, which contains authentication information. The Switch passes information to the configured Radius server, which can authenticate a user name and password before authorizing use of the network.

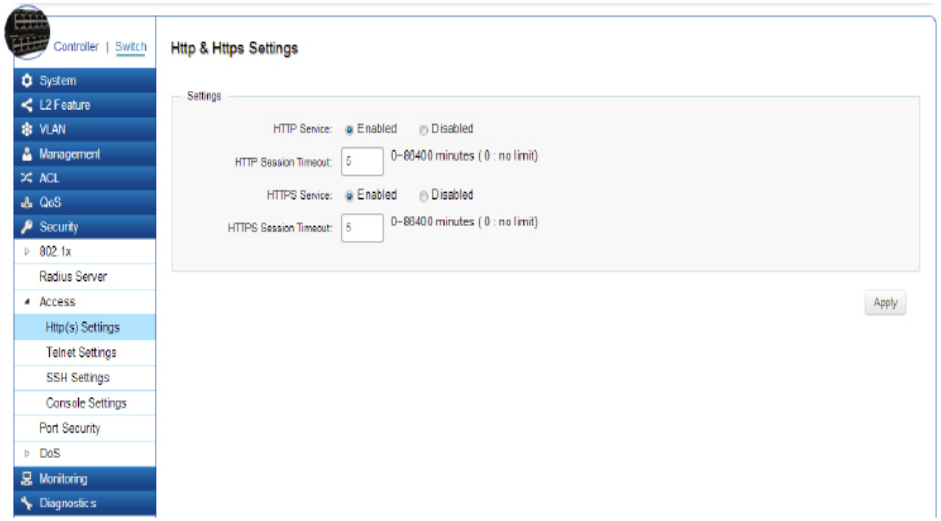
Index:	Displays the index for which RADIUS Server is displayed.
Server IP:	Enter the RADIUS Server IP address.
Authorized Port:	Enter the authorized port number. The default port is 1812.
Accounting Port:	Enter the name you wish to use to identify this Switch.
Key String:	Enter the Key String used for encrypting all RADIUS communication between the device and the RADIUS server.
Timeout Reply:	Enter the amount of time the device waits for an answer from the RADIUS Server before switching to the next server. The default value is 3.
Retry:	Enter the number of transmitted requests sent to the RADIUS server before a failure occurs. The default is 3.
Server Priority:	Enter the priority for the RADIUS server.
Dead Timeout:	Enter the amount of time that the RADIUS Server is bypassed for service requests. The default value is 0.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Access

Http & Https Settings

The EnGenius Layer 2 PoE+ Switch provides a built-in browser interface that enables you to configure and manage the Switch via Hypertext Transfer Protocol (Http) and Hypertext Transfer Protocol Secure (Https) requests selectivly to help prevent security breaches on the network. You can manage your HTTP and HHTPs settings for the Switch further by choosing the length of session timeouts for HTTP and HTTPs requests. Select whether to **Enable** or **Disable** the HTTP service and enter the HTTP Timeout session. Next, select whether to **Enable** or **Disable** the HTTPS sevice and enter the HTTPS timeout session for the Switch.

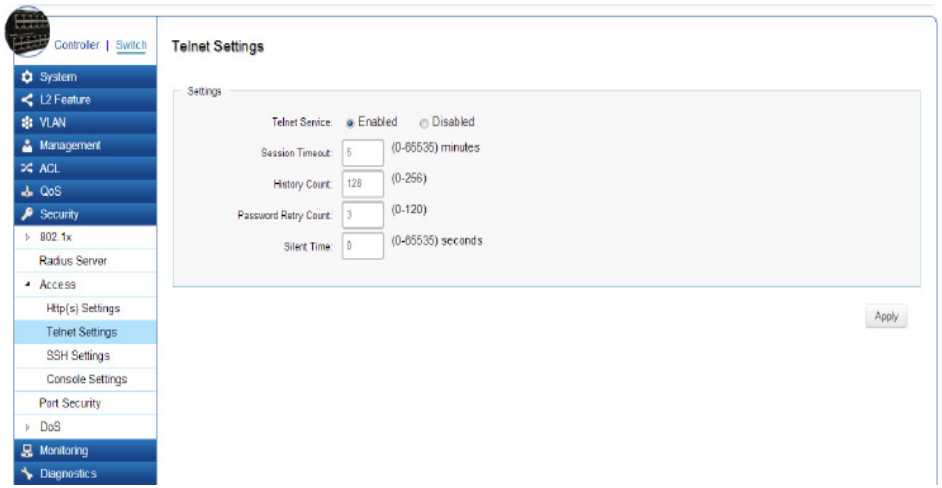


HTTP Service:	Select whether HTTP Service for the Switch is **Enabled** or **Disabled**. This is enabled by default.
HTTP Session Timeout:	Enter the amount of time that elapses before HTTP is timed out. The default is 5 minutes. The range is from 0-86400 minutes.
HTTPS Service:	Select whether the HTTP Service is **Enabled** or **Disabled.** This is disabled by default.
HTTPS Session Timeout:	Enter the amount of time that elapses before HTTPS is timed out. The default is 5 minutes. The range is from from 0-86400 minutes.

Click **Apply** to save the changes to the system.

Telnet Settings

From here, you can configure and manage the Switch's Telnet protocol settings. The Telnet protocol is a standard internet protocol which enables terminals and applications to interface over the Internet with remote hosts by providing Command Line Interface (CLI) communication using a virtual terminal connection. This protocol provides the basic rules for making it possible to link a client to a command interpreter. The Telnet service for the Switch is enabled by default. Please note that for secure communication, it is better to use SSH over Telnet. To enable and configure SSH Settings, please refer to SSH Settings on the next page.

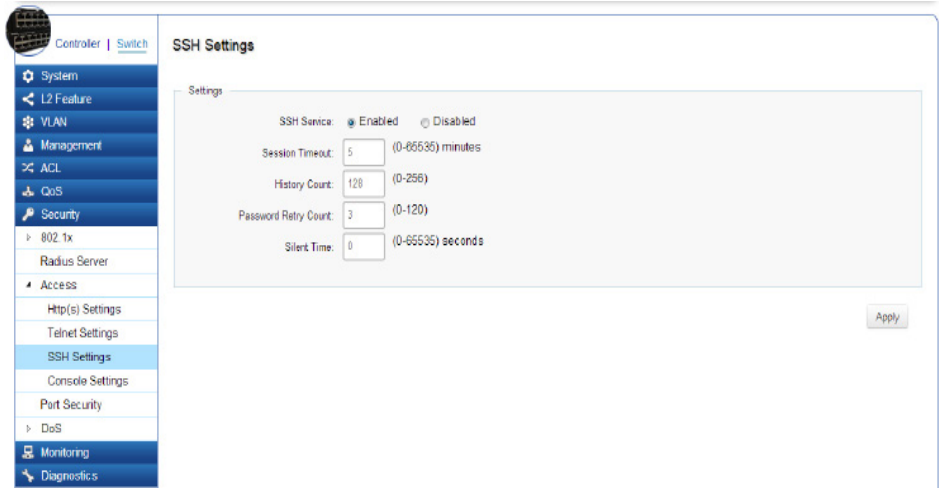


Telnet Service:	Select whether the Telnet Service is **Enabled** or **Disabled**. It is enabled by default.
Session Timeout:	Enter the amount of time that elapses before the Telnet Service is timed out. The default is 5 minutes. The range is from 0-65535 minutes.
History Count:	Enter the entry number for History of Telnet Service. The default is 128. The range is from 0-256.
Password Retry Count:	Enter the number of password request send to Telnet Service. The default is 3. The range is from 0-120.
Silent Time:	Enter the silent time for Telnet Service. The range is from 0-65535 seconds.

Click **Apply** to save the changes to the system.

SSH Settings

Secure Shell (SSH) is a cryptographic network protocol for secure data communication network services. SSH is a way of accessing the command line interface on the network Switch.The traffic is encrypted, so it is difficult to eavesdrop on as it creates a secure connection within an insucure network such as the internet. Even if an attacker was able to view the traffic, the data would be incomprehensible without the correct encryption key to decode it.



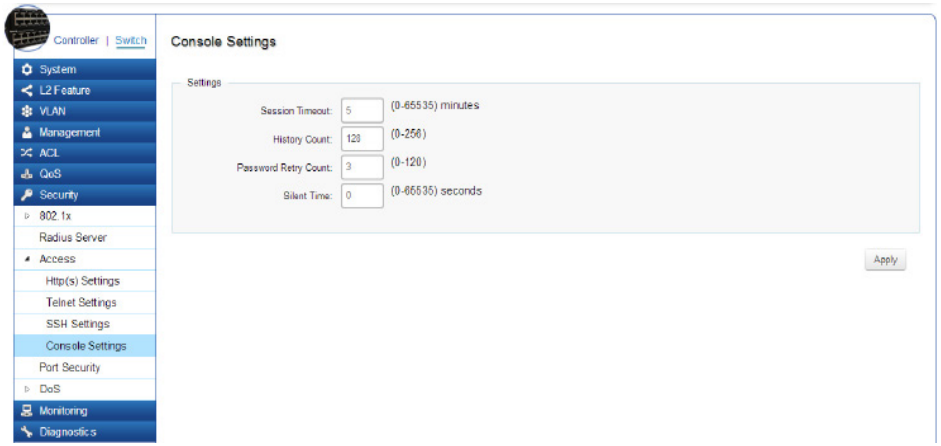
To configure SSH settings for the Switch, first select whether you wish to Enable or Disable the SSH service for the Switch. Note that SSH is more secure than the Telnet service when deciding between which service to use. Enter the session timout you wish to implement for SSH. Next, enter the History Count number you wish. The default count is: 128. Enter the number of passwords requests to be sent across SSH. The deafult attempts is: 3. Finally, enter the silent time you wish to implement for the SSH service.

SSH Service:	Select whether SSH is **Enabled** or **Disabled**. This is disabled by default.
Session Timeout:	Enter the amount of time that elapses before the SSH Service is timed out. The default is 5 minutes. The range is from 0-65535 minutes.
History Count:	Enter the entry number for History of SSH Service. The default is 128. The range is from 0-256.
Password Retry Count:	Enter the number of password request sent to the SSH Service. The default is 3. The range is from 0-120.
Silent Time:	Enter the silent time for SSH Service. The range is from 0-65535 seconds.

Click **Apply** to save the changes to the system.

Console Settings

From here, you can configure the Console Service settings for the Switch.

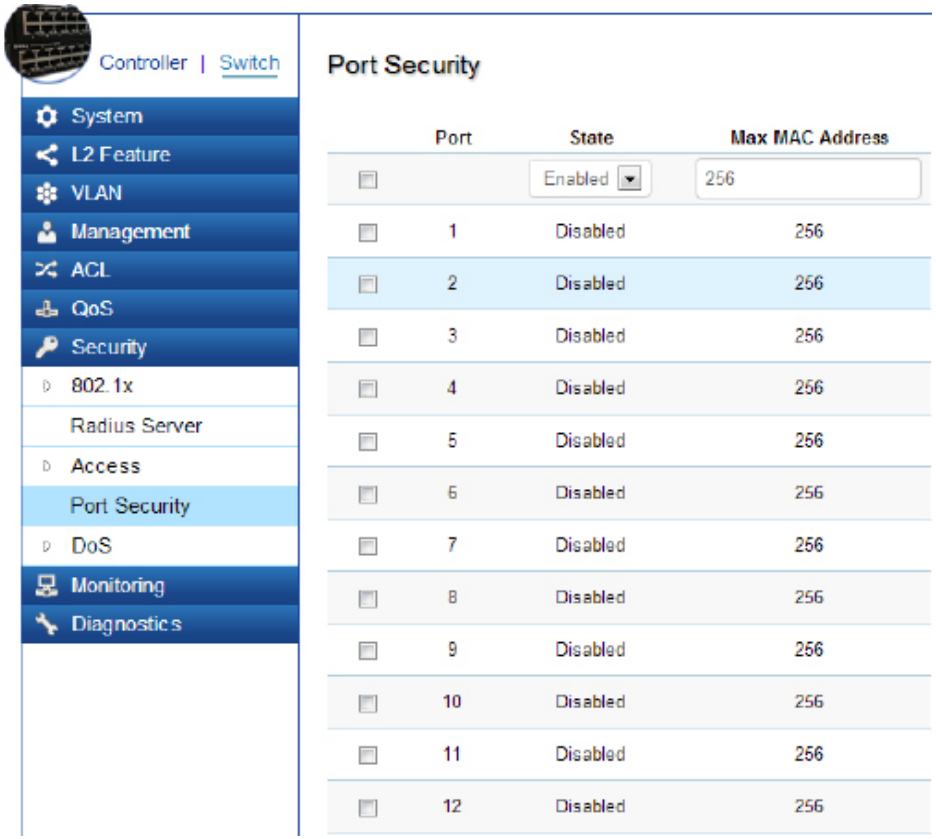


Session Timeout:	Enter the amount of time that elapses before Console Service is timed out. The default is 5 minutes. The range is from 0-65535 minutes.
History Count:	Enter the entry number for History of Console Service. The default is 128. The range is from 0-256.
Password Retry Count:	Enter the number of password requests to send to the Console Service. The default is 3. The range is from 0-120.
Silent Time:	Enter the silent time for Console Service. The range is from 0-65535 seconds.

Click **Apply** to save the changes to the system.

Port Security

Network security can be increased by limiting access on a specific port to users with specific MAC addresses. Port Security prevents unauthorized device to the Switch prior to stopping auto-learning processing.



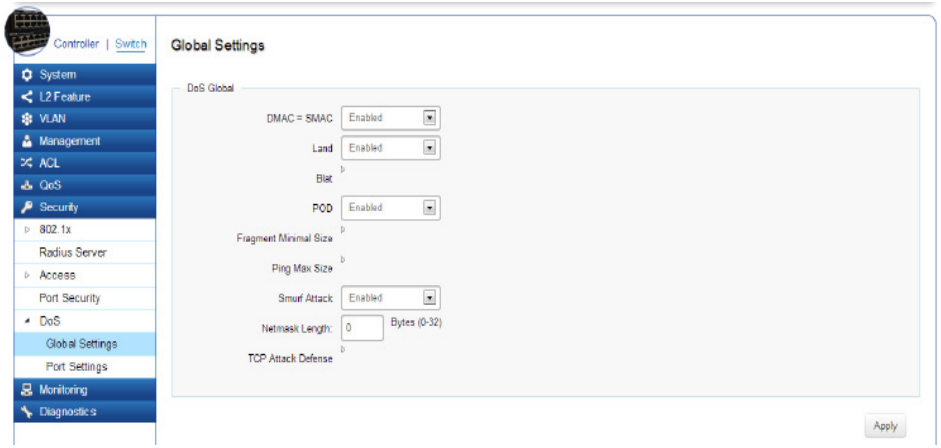
Max MAC Address:	Enter the maximum number of MAC Addresses that can be learned on the port. The range is from 1-256.
Port:	Displays the port for which the port security is defined.
State:	Select **Enabled** or **Disabled** for the port security feature for the selected port.

Click **Apply** to save the changes to the system.

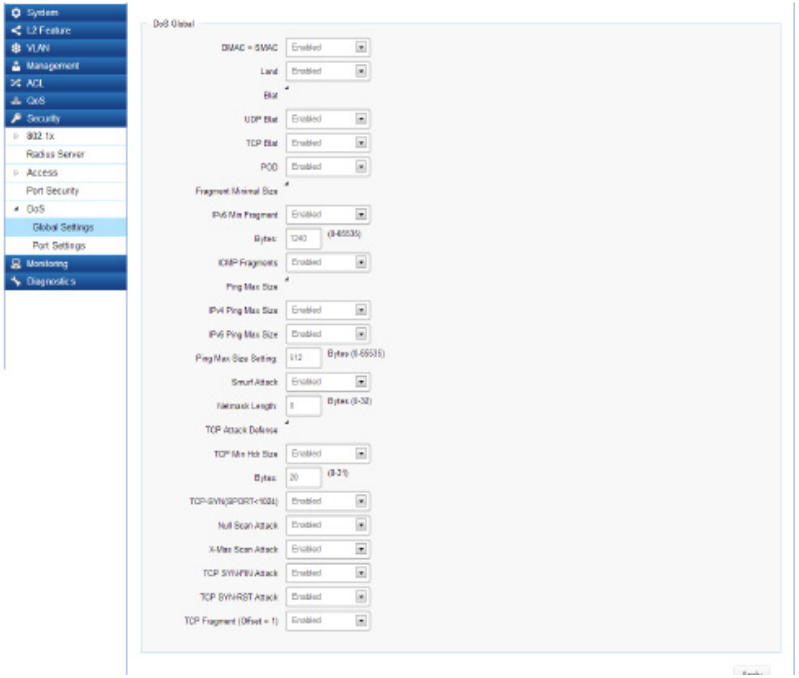
DoS

DoS (Denial of Service) is used for classifying and blocking specific types of DoS attacks. From here, you can configure the Switch to monitor and block different types of attacks:

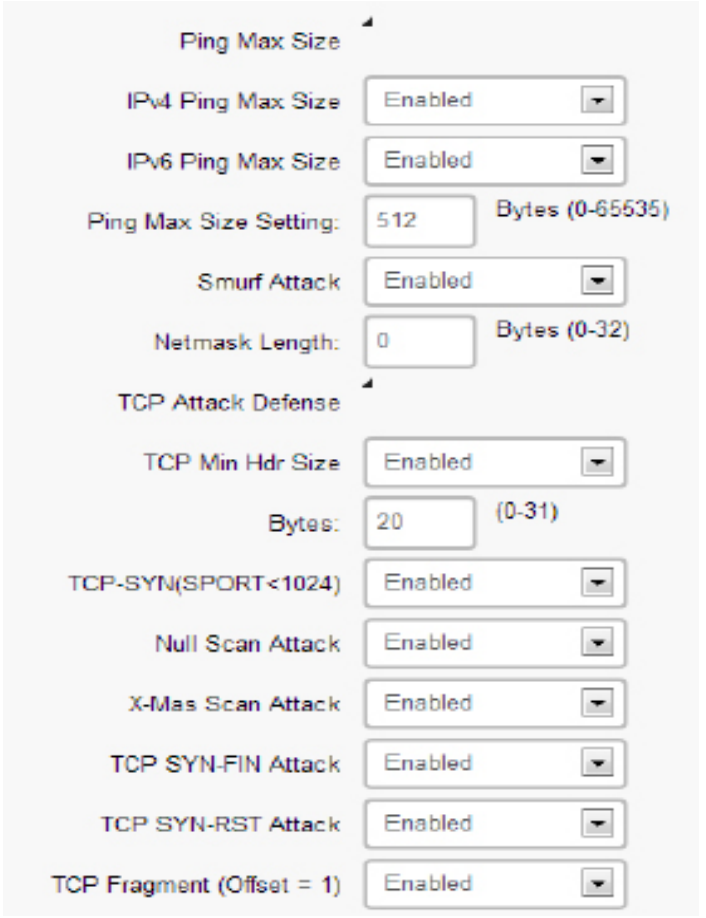
Global Settings



DMAC = SMAC:	Select **Enabled** or **Disabled** from the list.
Land:	Select **Enabled** or **Disabled** from the list.
UDP Blat:	Select **Enabled** or **Disabled** from the list.
TCP Blat:	Select the **Enabled** or **Disabled** from the list.
POD:	Select the **Enabled** or **Disable** from the list.
Fragment Minimal Size:	Enter the minimal size.
IPv6 Min Fragment:	Select **Enabled** or **Disabled** from the list.
Bytes:	Enter the size of IPv6 packets. The range is from 0-65535.
ICMP Fragment:	Select **Enabled** or **Disabled** from the list.



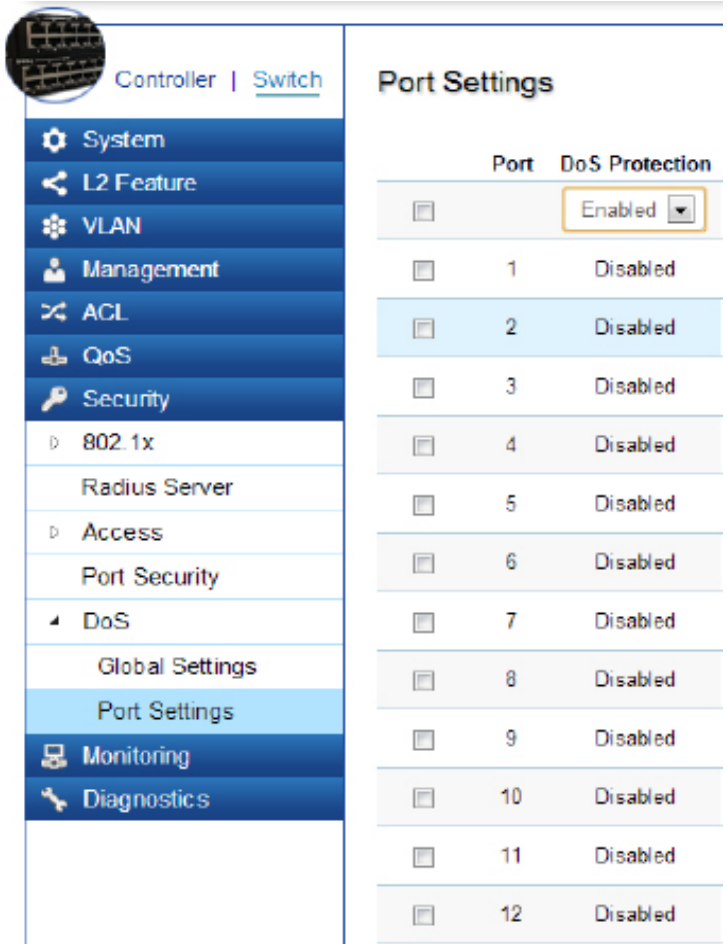
DMAC = SMAC:	Select **Enabled** or **Disabled** from the list.
Land:	Select **Enabled** or **Disabled** from the list.
UDP Blat:	Select **Enabled** or **Disabled** from the list.
TCP Blat:	Select the **Enabled** or **Disabled** from the list.
POD:	Select the **Enabled** or **Disable** from the list.
Fragment Minimal Size:	Enter the minimal size.
IPv6 Min Fragment:	Select **Enabled** or **Disabled** from the list.
Bytes:	Enter the size of IPv6 packets. The range is from 0-65535.
ICMP Fragment:	Select **Enabled** or **Disabled** from the list.
Ping Max Size:	Enter the max ping size you wish to use.
IPv4 Ping Max Size:	Select **Enabled** or **Disabled** from the list.
IPv6 Ping Max Size:	Select **Enabled** or **Disabled** from the list.
Ping Max Size Setting:	Enter the max ping size for the ping. The range is from 0-65535.
Smurf Attack:	Select **Enabled** or **Disabled** from the list.
Netmask Length:	Enter the length of the netmask. The range is from 0-32. **TCP-SYN:** Select **Enabled** or **Disabled** from the list.
Null Scan Attack:	Select **Enabled** or **Disabled** from the list.
X-Mas Scan Attack:	Select **Enabled** or **Disabled** from the list.
TCP SYN-FIN Attack:	Select **Enabled** or **Disabled** from the list.
TCP SYN-RST Attack:	Select **Enabled** or **Disabled** from the list.
TCP Fragment:	Select **Enabled** or **Disabled** from the list.



Click **Apply** to save the changes to the system.

Port Settings

From here you can configure the Port Settings for DoS for the Switch. Select from the drop down list whether you wish to **Enable** or **Disable** DoS Protection for the Switch.



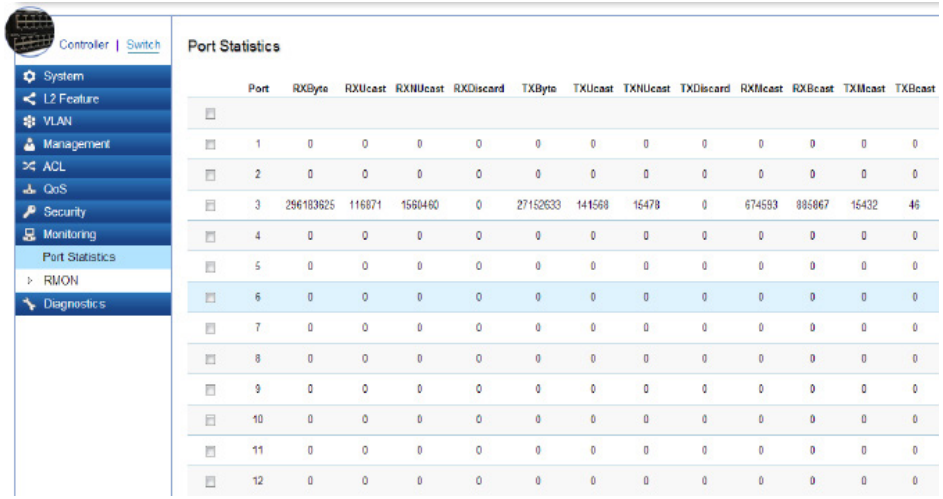
Port:	Displays the port for which the DoS protection is defined.
DoS Protection:	Select **Enabled** or **Disabled** for the DoS Protection feature for the selected port.

Click **Apply** to save the changes to the system.

Monitoring

Port Statistics

The Port Statistics section displays a summary of all port traffic statistics regarding the monitoring features on the Switch.



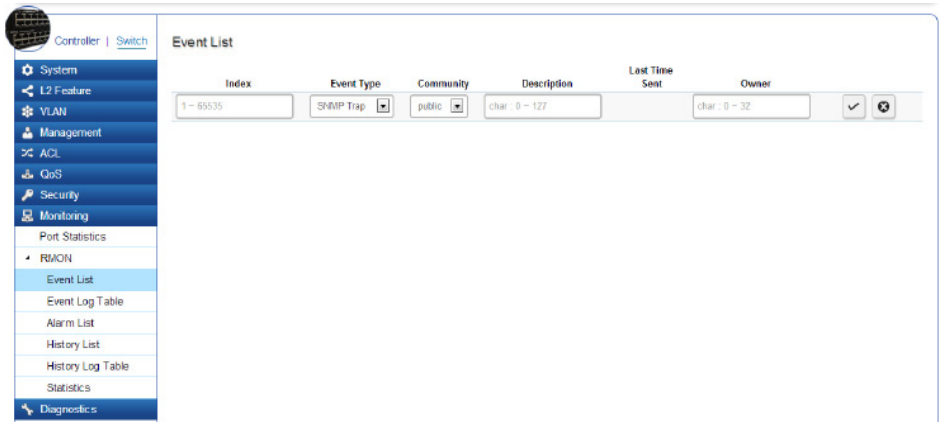
Port:	Displays the port for which statistics are displayed.
RXByte:	Displays the number of all packets received on the port.
RXUcast:	Displays the number of Unicast packets received on the port.
RXNUcast:	Displays the number of Unicast packets received on the port.
RXDiscard:	Displays the number of received packets discarded on the port.
TXByte:	Displays the number of all packets transmitted on the port.
TXUcast:	Displays the number of Unicast packets transmitted on port.
TXNUcast:	Displays the number of Unicast packets transmitted on the port.
TXDiscard:	Displays the number of transmitted packets discarded on the port.
RXMcast:	Displays the number of Multicast packets received on the port.
RXBcast:	Displays the number of Broadcast packets received on the port.
TXMcast:	Displays the number of Multicast packets transmitted on the port.
TXBcast:	Displays the number of Broadcast packets transmitted on the port.

RMON

Remote Network Monitoring, or RMON is used for support monitoring and protocol analysis of LANS by enabling various network monitors and console systems to exchange network-monitoring data through the Switch.

Event List

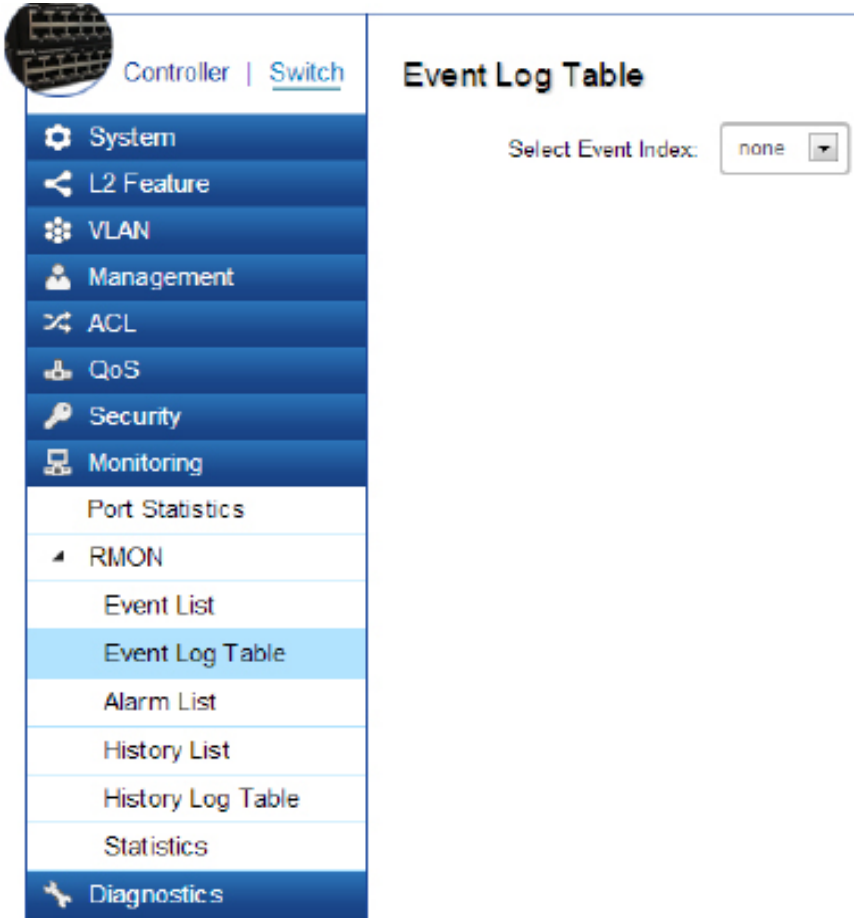
The Event List defines RMON events on the Switch.



Index:	Enter the entry number for Event.
Event Type:	Select the event type. • **Log** - The event is a log entry. • **SNMP Trap** - The event is a trap. • **Log & Trap** - The event is both a log entry and a trap.
Community:	Enter the community to which the event belogs.
Description:	Displays the number of good broadcast packets received on the interface.
Last Time Sent:	Displays the time that event occurred. Owner: Enter the switch that defined the event.

Event Log Table

From here, you can view specific Event logs for the Switch. Choose an Event log you wish to view fromt he drop-down list.

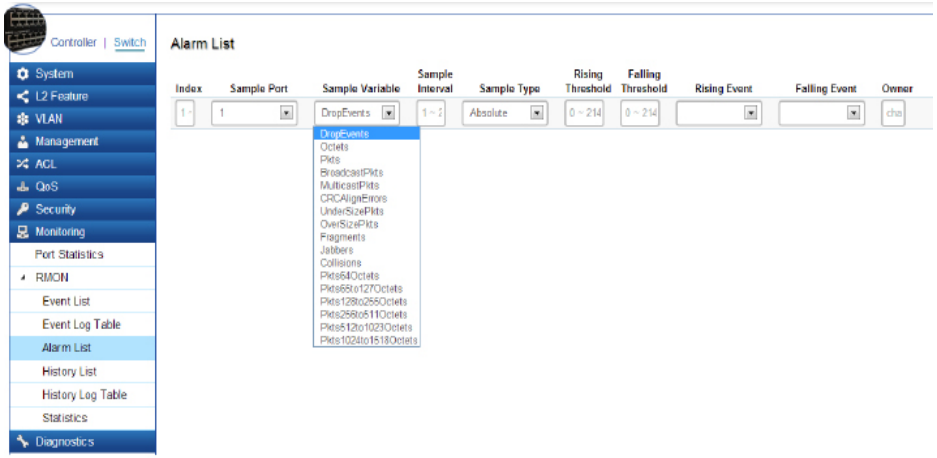


Event Log Table:	Select the index of the Event Log from the list.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Alarm List

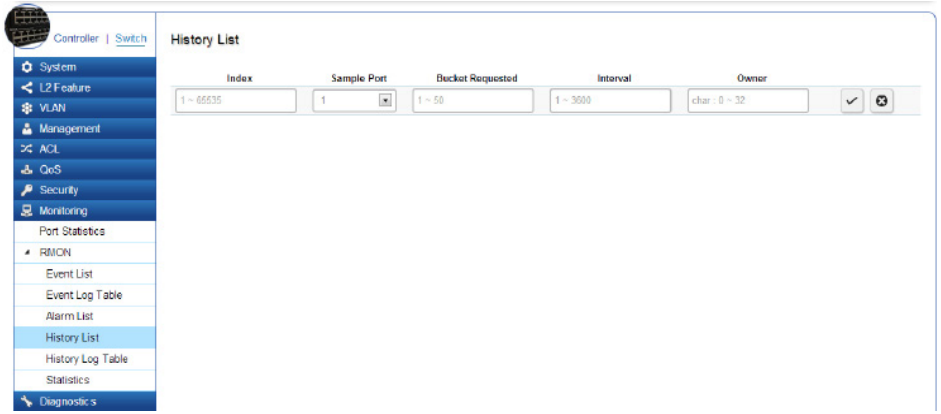
You can configure Network alarms to occur when a network problem is detected. Choose your preferences for the alarm from the drop-down boxes.



Index:	Enter the entry number for the History Log Table. Sample Port: Select the port from which the alarm samples were taken.
Sample Variable:	Select the variable of samples for the specified alarm sample.
Sample Interval:	Enter the alarm interval time.
Sample Type:	Select the sampling method for the selected variable and comparing the value against the thresholds. • **Absolute -** Compares the values with the thresholds at the end of the sampling interval. • **Delta -** Subtracts the last sampled value from the current value.
Rising Threshold:	Enter the rising number that triggers the rising threshold alarm.
Falling Threshold:	Enter the falling number that triggers the falling threshold alarm
Rising Event:	Enter the event number by the falling alarm are reported.
Falling Event:	Enter the event number by the falling alarms are reported.
Owner:	Enter the Switch that defined the alarm.

History List

The RMON History List screen contains information about samples of data taken from the ports.



Index:	Enter the entry number for the History Log Table.
Sample Port:	Select the port from which the history samples were taken.
Bucket Requested:	Enter the number of samples to be saved. The range is from 1- 50.
Interval:	Enter the time that samples are taken from the ports. The field range is from 1-3600.
Owner:	Enter the RMON user that requested the RMON information. The range is from 0-32 characters.

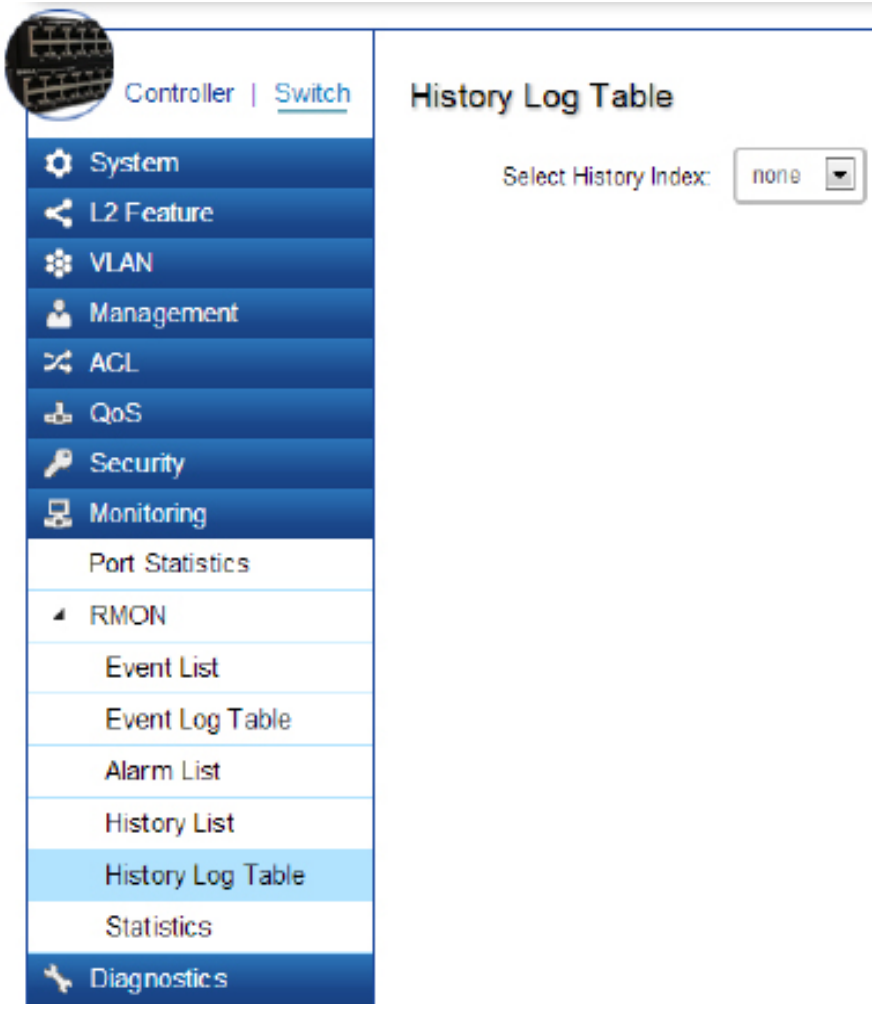
Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

I

History Log Table

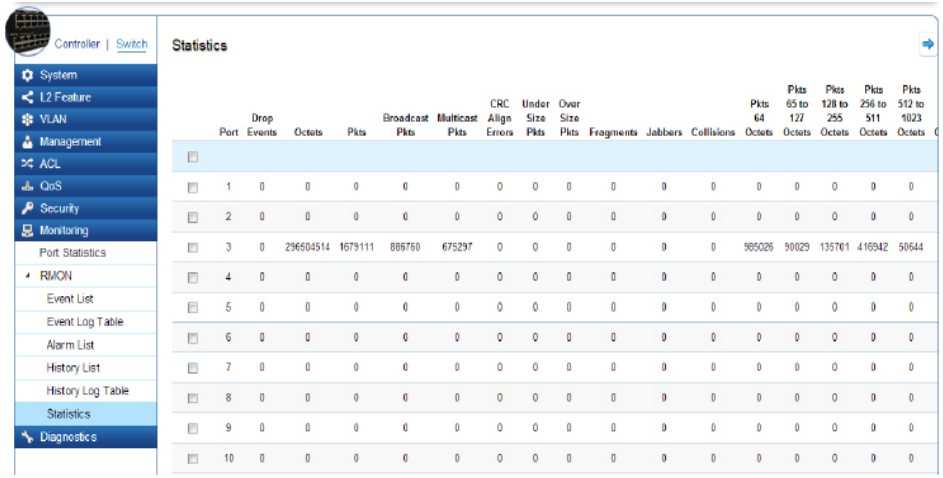
From here, you can view the History Index for History Logs on the Switch. Select a History Index to view from the drop-down box.

History Log Table:	Select the index for the History Log from the list.



Statistics

From here, you can view all the packet information for the controller feature of the Switch.



Port:	Select the specific port for which RMON statistics are displayed.
Drop Events:	Displays the number of dropped events that have occurred on the port.
Octets:	Displays the sample number from which the statistic taken.
Pkts:	Displays the number of octets received on the port.
Broadcast Pkts:	Displays the number of good broadcast packets received on the port. This number does not include Multicast packets.
Multicast Pkts:	Displays the number of good Multicast packets received on the port.
CRC & Align Errors:	Displays the number of CRC and Align errors that have occurred on the port.
Undersize Pkts:	Displays the number of undersized packets (less than 64 octets) received on the port.
Oversize Pkts:	Displays the number of oversized packets (over 1518 octets) received on the port.
Fragments:	Displays the number of fragments received on the port.
Jabbers:	Displays the total number of received packets that were longer than 1518 octets.
Collisions:	Displays the number of collisions received on the port.
Pkts of 64 Octets:	Displays the number of 64-byte frames received on the port.
Pkts of 65 to 127 Octets:	Displays the number of 65 to 127 byte packets received on the port.
Pkts of 128 to 255 Octets:	Displays the number of 128 to 255 byte packets received on the port.
Pkts of 256 to 511 Octets:	Displays the number of 256 to 511 byte packets received on the port.
Pkts of 512 to 1023 Octets:	Displays the number of 512 to 1023 byte packets received on the port.
Pkts of 1024 to 1522 Octets:	Displays the number of 1024 to 1522 byte packets received on port.

Log

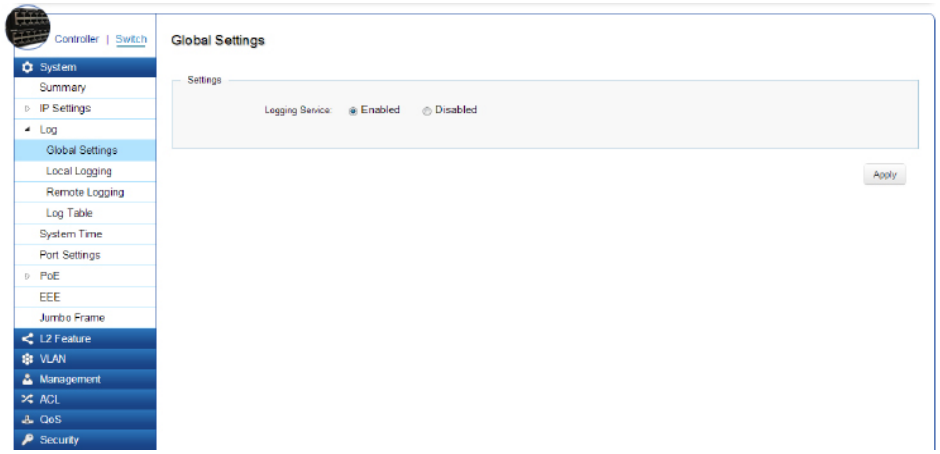
The Syslog Protocol allows devices to send event notification messages in response to events, faults, or errors occurring on the platform as well as changes in configuration or other occurrences across an IP network to syslog servers. It then collects the event messages, providing powerful support for users to monitor network operation and diagnose malfunctions. A Syslog-enabled device can generate a syslog message and send it to a Syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content, and system log related information of Syslog messages. Each Syslog message has a facility and severity level. The Syslog facility identifies a file in the Syslog server. Refer to the documentation of your Syslog program for details. The following table describes the Syslog severity levels.

Code	Severity	Description	General Description
0	Emergency	System is unusable	A emergency condition usually affecting multiple apps/servers/sites. Direct Attention is required.
1	Alert	Actions must be taken immediately	Should be corrected immediately. Notify staff who can fix the problem promptly.
2	Critical	Critical conditions	Should be corrected immediately, but indicates failure in a secondary system.
3	Error	Error conditions	Non-urgent failures, these should be relayed to developers or admins; each item should be resolved promptly.
4	Warning	Warning conditions	Warning message that indicates an error will occur if action is not taken.
5	Notice	Normal but significant conditions	Events that are unusual but not error inducing. No immediate action required.
6	Informational	Informational message	Normal operational status may be gained for reporting procedures.
7	Debug	Debug-level messages	Information useful to developers for debugging applications.

Global Settings

From here, you can **Enable** or **Disable** the Log settings for the Switch.



Logging Service:	Use the radio buttons to **Enable** or **Disable** the system log.
Global Logs:	Select whether to **Enable** or **Disable** the Switch's global logs for Cache, File, and Server Log.

Apply: Click **APPLY** to update the system settings.

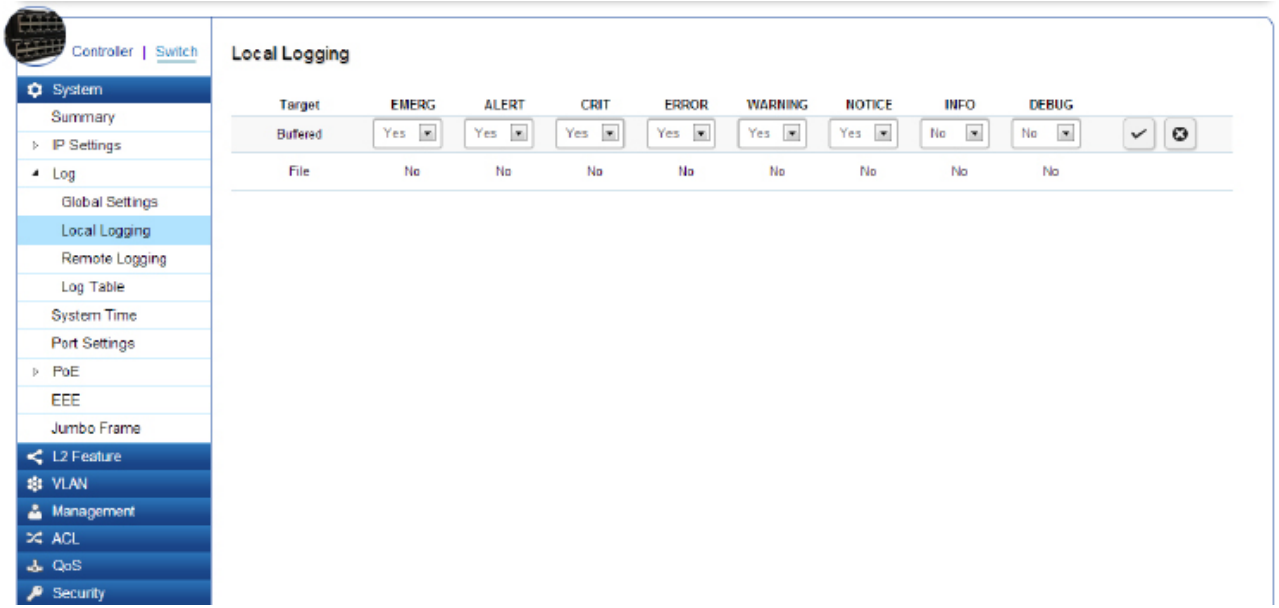
Local Logging

From here, you can discover the paths that a packet takes to a destination. The Switch supports log output to two directions: **Flash** and **RAM**. The information stored in the system's Flash log will be lost after the Switch is rebooted or powered off, whereas the information stored in the system's RAM will be kept effective even if the Switch is rebooted or powered off.

Target:	The method for saving the Switch log, to Flash, RAM or both.
Flash:	Log erased after reboot or power off
RAM:	Log stored in RAM. Will only be erased after system reset.
Severity Level:	Refer to severity level table.

Logs with the selected severity level and all logs of greater severity are sent to the host. For example, if you select **Error**, the logged messages include **Error, Critical, Alert,** and **Emergency.**

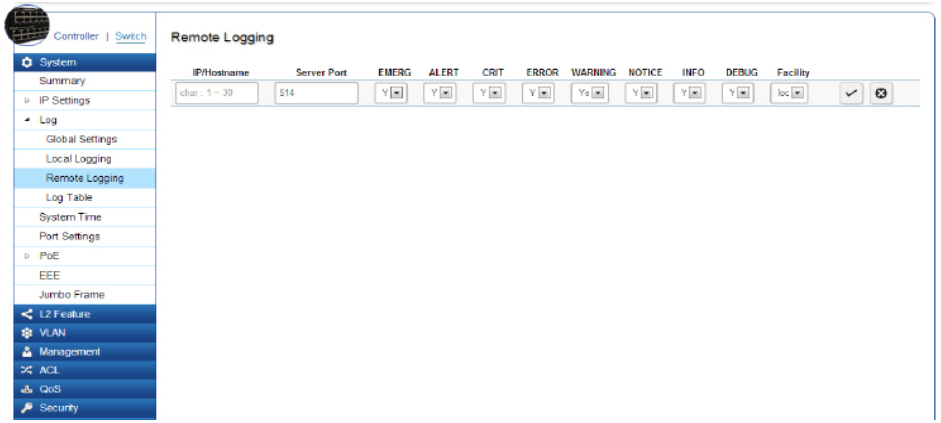
Target:	Select **Yes** or **No** from the list. If the device is not functioning properly, an emergency log message is saved to the specified logging location.
EMERG:	Select **Yes** or **No** from the list. If the Switch is not functioning properly, an emergency log message is saved to the specified logging location.
ALERT:	Select **Yes** or **No** from the list. If there is a serious Switch malfunction, then all Switch features are down.
CRIT:	Select **Yes** or **No** from the list. A critical log is saved if a critical Switch malfunction occurs.
ERROR:	Select **Yes** or **No** from the list. If triggered, a device error has occurred.
WARNING:	Select **Yes** or **No** from the list. The device is functioning, but an operational problem has occurred.
NOTICE:	Select **Yes** or **No** from the list. This will provide information about the Switch.
INFO:	Select **Yes** or **No** from the list. This will provide information about the Switch.
DEBUG:	Select whether the **Yes** or **No** from the list. This will provide a debugging message.



Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Remote Logging

From here, you can discover the paths that a packet takes to a destination. Remote logging enables the Switch to send system logs to the Log Server. The Log Server helps to centralize system logs from various devices such as Access Points so that the user can monitor and manage the whole network. Click the **Add** button and select the severity level of events you wish to log.

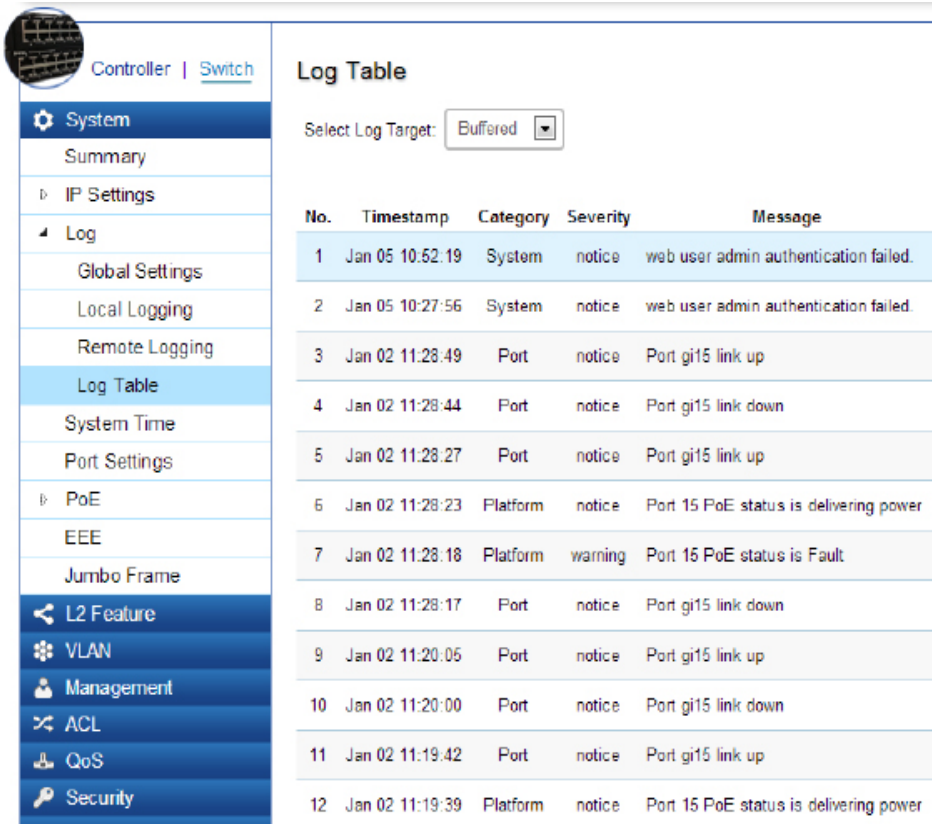


IP/Hostname:	Specify the IP address or host name of the host configured for the Syslog.
Server Port:	Specify the port on the host to which Syslog messages are sent. The default port is 514.
Severity Level:	Refer to severity level table on page 25 or 27. Logs with the selected severity level and all logs of greater severity are sent to the host. For example, if you select Error, the logged messages include Error, Critical, Alert, and Emergency
Facility:	The log facility is used to separate out log messages by application or by function, allowing you to send logs to different files in the syslog server. Use the drop-down menu to select local0, local1, local2, local3, local4, local5, local6, or local7.

Click the **Apply** button to accept the changes or the **Cancel** button to discard them.

Log Table

From here, users can view and delete the history log. Select the Log Target you wish to view from the drop-down box.


Controller | Switch
System
Summary
IP Settings
Log
Global Settings
Local Logging
Remote Logging
Log Table
System Time
Port Settings
PoE
EEE
Jumbo Frame
L2 Feature
VLAN
Management
ACL
QoS
Security
Log Table
Select Log Target: Buffered
No. Timestamp Category Severity Message
1 Jan 05 10:52:19 System notice web user admin authentication failed.
2 Jan 05 10:27:56 System notice web user admin authentication failed.
3 Jan 02 11:28:49 Port notice Port gi15 link up
4 Jan 02 11:28:44 Port notice Port gi15 link down
5 Jan 02 11:28:27 Port notice Port gi15 link up
6 Jan 02 11:28:23 Platform notice Port 15 PoE status is delivering power
7 Jan 02 11:28:18 Platform warning Port 15 PoE status is Fault
8 Jan 02 11:28:17 Port notice Port gi15 link down
9 Jan 02 11:20:05 Port notice Port gi15 link up
10 Jan 02 11:20:00 Port notice Port gi15 link down
11 Jan 02 11:19:42 Port notice Port gi15 link up
12 Jan 02 11:19:39 Platform notice Port 15 PoE status is delivering power

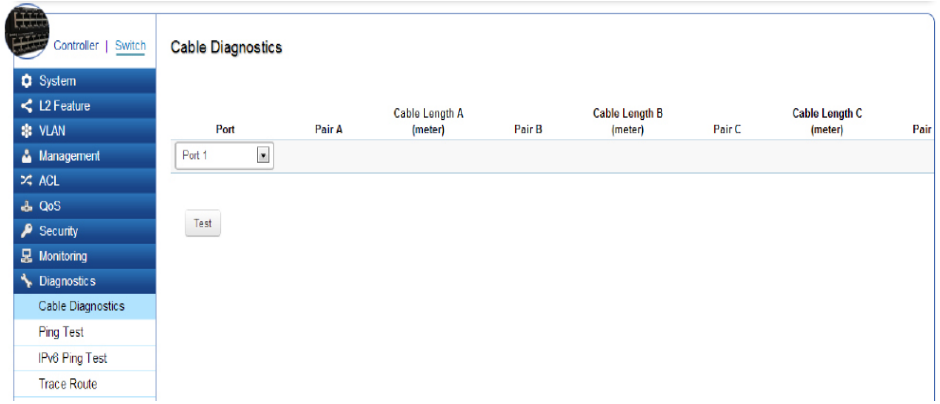
No.:	A counter incremented whenever an entry to the Switch's history log is made. It displays the last entry (highest sequence number) first.
Timestamp:	Displays the time of the log entry.
Category:	Displays the category of the history log entry. for example, If the name of a VLAN group is changed, the category will display "VLAN". If a device is connected to the Switch, the category will display "Port".
Severity:	Displays the level of severity of the log entry. Messages are assigned a severity code.
Message:	Displays text describing the event that triggered the history log entry.

Click **CLEAR** to clear the buffered log in the memory.

Diagnostics

Cable Diagnostics

Cable Diagnostics helps you to detect whether your cable has connectivity problems provides information about where errors have occurred in the cable. The tests use Time Domain Reflectometry (TDR) technology to test the quality of a copper cable attached to a port. TDR detects a cable fault by sending a signal through the cable and reading the signal that is reflected back. All or part of the signal is reflected back either by cable defects or by the end of the cable when an issue is present. Cables are tested when the ports are in the down state, with the exception of the cable length test.



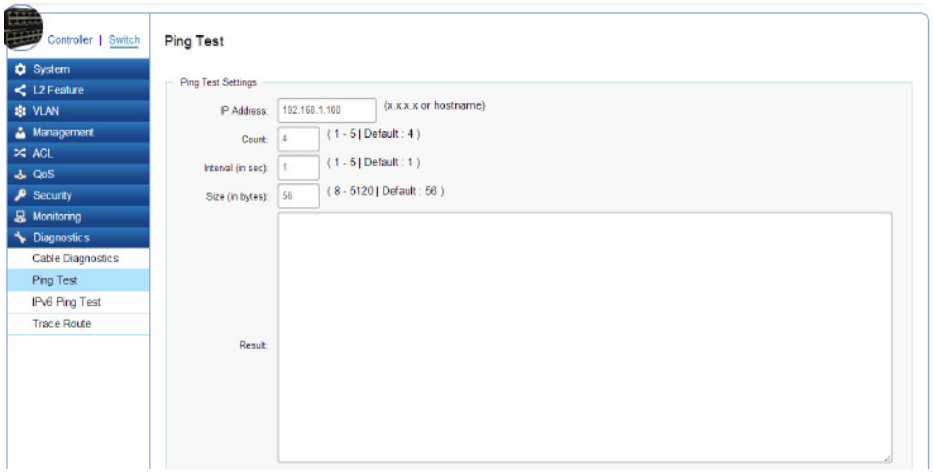
Port:	Select the port to which the cable is connected. Pair (A, B, C, and D): Displays the cable test results. • **Open** – A cable is not connected to the port. • **OK** – A cable is connected to the port.
Cable Length (A, B, C, and D):	Displays the approximate cable length.

To verify accuracy of the test, it is reccomended that you run multiple tests in case of a test fault or user error.

Click **Test** to perform the cable tests for the selected port.

Ping Test

The Packet INternet Groper (Ping)Test allows you to verify connectivity to remote hosts. The Ping test operates by sending Internet Control Message Protocol (ICMP) request packets to the tested host and waits for an ICMP response. In the process it measures the time from transmission to reception and records any packet loss.Send a ping request to a specified IPv4 address. Check whether the Switch can communicate with a particular network host before testing.



Ping Test Settings

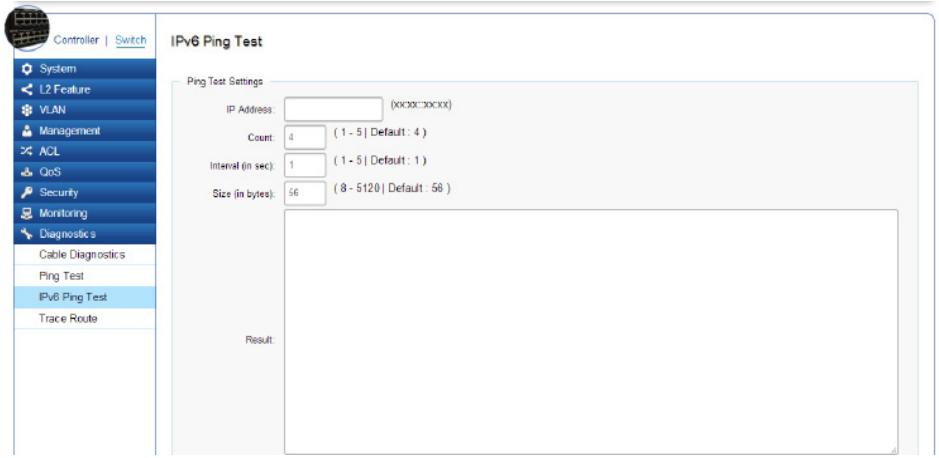
You can vary the test parameters by entering the data in the appropraite boxes. To verify accuracy of the test, it is reccomended that you run multiple tests in case of a test fault or user error.

IP address:	Enter the IP address or the host name of the station you want the Switch to ping to.
Count:	Enter the number of ping to send. The range is from 1-5 and the default is 1.
Interval:	Enter the number of seconds between pings sent. The range is from 1-5 and the default is 4.
Size:	Enter the size of ping packet to send. The range is from 8-5120 and the default is 56.
Result:	Displays the ping test results.

Click **Test** to perform the ping tests.

IPv6 Ping Test

Send a ping request to a specified IPv6 address. Check whether the Switch can communicate with a particular network host before testing.



You can vary the test parameters by entering the data in the appropraite boxes. To verify accuracy of the test, it is reccomended that you run multiple tests in case of a test fault or user error.

IP address:	Enter the IPv6 address or the host name of the station you want the Switch to ping to.
Count:	Enter the number of pings to send. The range is from 1-5 and the default is 1.
Interval:	Enter the number of seconds between pings sent. The range is from 1-5 and the default is 4.
Size:	Enter the size of ping packet you wish to send. The range is from 8-5120 and the default is 56.
Result:	Displays the ping test results.

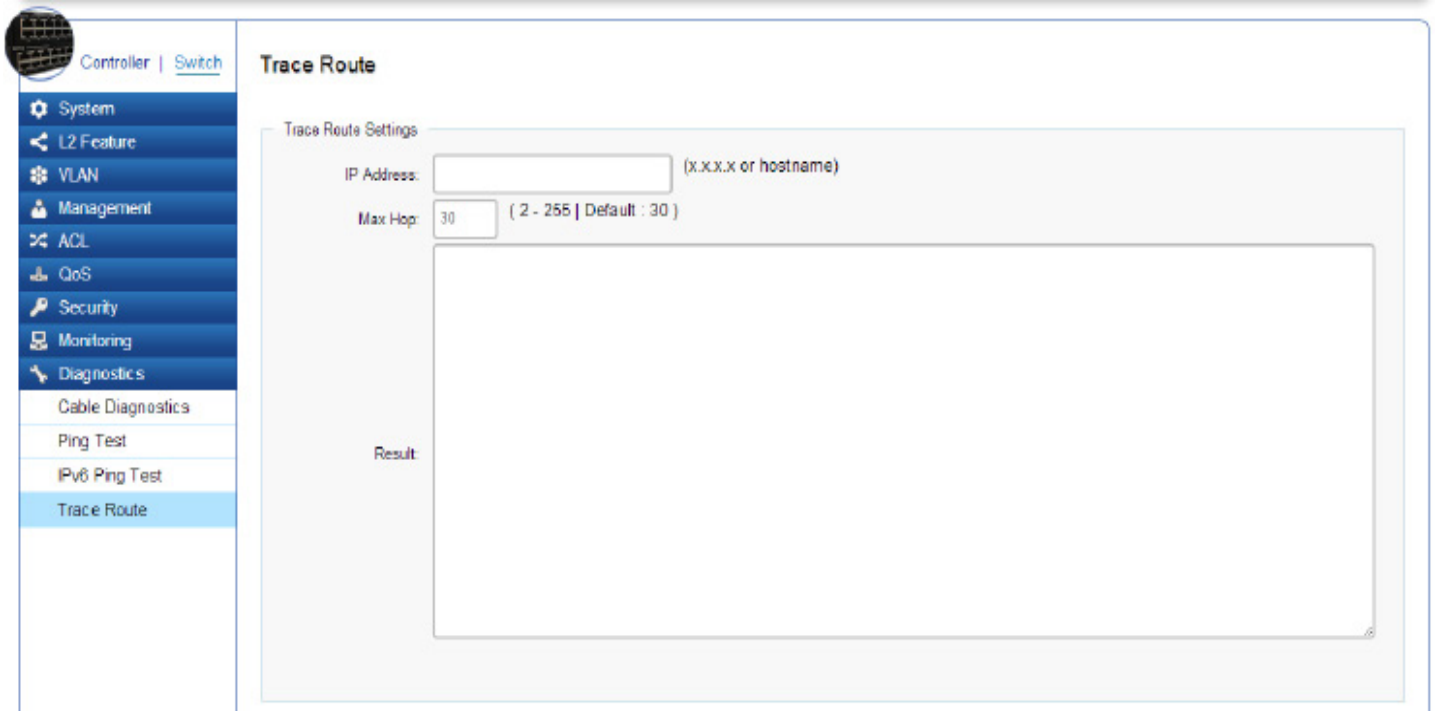
Click **Test** to perform the ping tests.

Trace Route

The traceroute feature is used to discover the routes that packets take when traveling to their destination. It will list all the routers it passes through until it reaches its destination, or fails to reach the destination and is discarded. In testing, it will tell you how long each hop from router to router takes via the trip time of the packets it sends and receives from each successive host in the route.

IP address:	Enter the IP address or the host name of the station you wish the Switch to ping to.
Max Hop:	Enter the maximum number of hops. The range is from 2-255 and the default is 30.
Result:	Displays the trace route results.

Click **Test** to initiate the trace route.



Chapter 4
Maintenance

Maintenance

Maintenance functions are available from the maintenance bar. Maintenance functions include: saving configuration settings, upgrading firmware, resetting the configuration to factory default standards, rebooting the device, and logging out of the interface.

The following represents the Maintenance Menu bar.

Saving Configurations

Important: You must save any setting changes before rebooting. Failure to save results in loss of new configuration changes.

Follow this procedure to save the configuration,

1. Click Save to save the entire configuration changes you have made to the device to Switch.
2. Click **OK**.

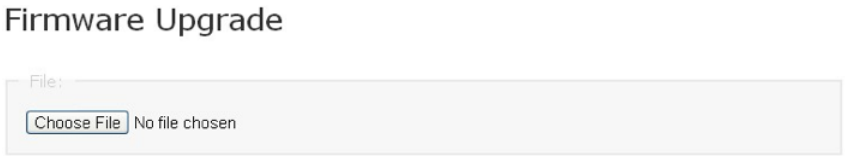
Upgrading

WARNING! Backup your configuration information before upgrading to prevent loss of settings information.

Follow this procedure to upgrade the Firmware.

1. Click Upgrade to start upgrading.

1. Click **Choose File**. When a window opens, browse to the location of your new Firmware.



3. Select the new Firmware file and click **OK**.

4. A prompt will displays to confirm the Firmware Upgrade. Click **OK** and follow the on-screen instructions to complete the Firmware Upgrade.

   Note: The Upgrade process may require a few minutes to complete. It is advised to clear your browser cache after upgrading your firmware.

Resetting

WARNING! The Reset function will delete all configuration information from the current device. Backup your information before starting this procedure.

Follow this procedure to reset the Switch back to factory default settings.

1. Click Reset to start the reset process.

2. When a prompt displays, click **OK** to confirm the reset or **Cancel** to quit the procedure.

Rebooting

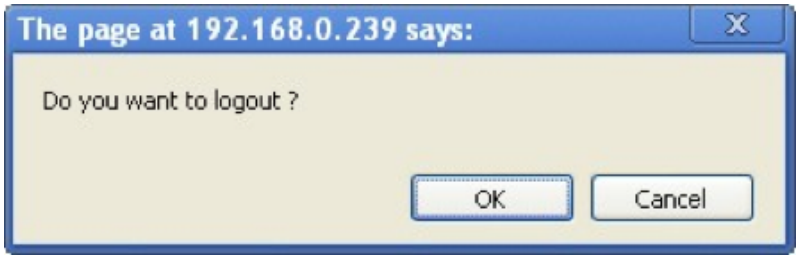
Follow this procedure to reboot the Switch.

1. Click Reboot to start the reboot process.
2. When a prompt displays, click **OK** to confirm the reboot process or **Cancel** to quit the procedure.

Logging Out

Follow this procedure to log out the current profile from the user interface.

1. Click Logout to log out of the menu.
2. When a prompt shows, click **OK** to confirm logging out or **Cancel** to quit the procedure.



Appendix

Quick Reference Guide

Hardware Specifications				
Model		**EWS5912FP**	**EWS7928P**	**EWS7952FP**
Connectors	Gigabit RJ45 Ports	10	24	48
	Gigabit SFP Ports	2	4	4
	Console Port	1	1	1
PoE Features	Standard	IEEE802.3af/at (max 30w per port)		
	PoE Ports	8	24	48
	Total PoE Budget	130 W	185 W	740 W
Power Supply		100-240VAC, 50/60Hz		
Environent		Operating Temperature: 32° F~122° F, 0° F -C~50° C Storage Temperature: -40° F~158° F, -40° C~70° C Operating Humidity: 10%~90% (non-condensing) Storage Humidity: 5%~90% (non-condensing)		
Dimensions		330 x 230 x 44mm (13 x 9 x 1.73 inches)	440 x 260 x 44mm (17.3 x 10.2 x 1.73 inches)	440 x 410 x 44mm (17.3 x 16.1 x 1.73 inches)"

WARNING!

This switch should be connected only to PoE networks without routing to the outside plant.

Professional Installation Instruction

1. Installation Personnel

This product is designed for specific application and needs to be installed by a qualified personnel who has RF and related rule knowledge. The general user shall not attempt to install or change the setting.

2. Installation Location

The product shall be installed at a location where the radiating antenna can be kept at least 23cm from nearby persons in normal operating conditions to meet regulatory RF exposure requirement.

3. External Antenna

Only use the antennas which have been approved by the applicant. Any non-approved antenna(s) may produce unwanted spurious or excessive RF transmitting power which may lead to the violation of FCC/IC limit and therefore is prohibited.

4. Installation Procedure

Please refer to the user's manual for details.

5. Warning!

Please carefully select the installation position and make sure that the final output power does not exceed the limit set force in relevant rules. The violation of this rule could lead to serious federal penalties.

Instructions D'installation Professionnelle

1. Installation

Ce produit est destine a un usage specifique et doit etre installe par un personnel qualifie maitrisant les radiofrequences et les regles s'y rapportant. L'installation et les reglages ne doivent pas etre modifies par l'utilisateur final.

2. Emplacement D'installation

En usage normal, afin de respecter les exigences reglementaires concernant l'exposition aux radiofrequences, ce produit doit etre installe de facon a respecter une distance de 23cm entre l'antenne emettrice et les personnes.

3. Antenn Externe.

Utiliser uniiquement les antennes approuvees par le fabricant. L'utilisation d'autres antennes peut conduire a un niveau de rayonnement essentiel ou non essentiel depassant les niveaux limites definis par FCC/IC, ce qui est interdit.

4. Procedure D'installation

Consulter le manuel d'utilisation.

5. Avertissement!

Choisir avec soin la position d'installation et s'assurer que la puissance de sortie ne depasse pas les limites en vigueur. La violation de cette regle peut conduire a de serieuses penalites federales.

Appendix A

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

WARNING!

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the fol- lowing two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Radiation Exposure Statement

WARNING! This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 23cm between the radiator & your body.

Appendix B - IC Interference Statement

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Caution:

(i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

(ii) high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

Avertissement:

(i) les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

(ii) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

FOR MOBILE DEVICE USAGE
Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Pour l'utilisation de dispositifs mobiles)
Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20cm de distance entre la source de rayonnement et votre corps.

Appendix C - CE Interference Statement

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- **EN60950-1**
  Safety of Information Technology Equipment
- **EN50385**
  Generic standard to demonstrate the compliance of electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic fields (0 Hz - 300 GHz)
- **EN 300 328**
  Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
- **EN 301 893**
  Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive
- **EN 301 489-1**
  Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
- **EN 301 489-17**
  Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

This device is a 5GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

CE 0560 !

Česky [Czech]	[Jméno výrobce] tímto prohlašuje, že tento [typ zařízení] je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede [fabrikantens navn] erklærer herved, at følgende udstyr [udstyrets typebetegnelse] overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt [Name des Herstellers], dass sich das Gerät [Gerätetyp] in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab [tootja nimi = name of manufacturer] seadme [seadme tüüp = type of equipment] vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, [name of manufacturer], declares that this [type of equipment] is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente [nombre del fabricante] declara que el [clase de equipo] cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ [name of manufacturer] ΔΗΛΩΝΕΙ ΟΤΙ [type of equipment] ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.

Français [French]	Par la présente [nom du fabricant] déclare que l'appareil [type d'appareil] est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente [nome del costruttore] dichiara che questo [tipo di apparecchio] è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo [name of manufacturer / izgatavotāja nosaukums] deklarē, ka [type of equipment / iekārtas tips] atbilst Direktīvas 1999/ 5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo [manufacturer name] deklaruoja, kad šis [equipment type] atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart [naam van de fabrikant] dat het toestel [type van toestel] in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, [isem tal-manifattur], jiddikjara li dan [il-mudel tal-prodott] jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, [gyártó neve] nyilatkozom, hogy a [... típus] megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym [nazwa producenta] oświadcza, że [nazwa wyrobu] jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	[Nome do fabricante] declara que este [tipo de equipamento] está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	[Ime proizvajalca] izjavlja, da je ta [tip opreme] v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	[Meno výrobcu] týmto vyhlasuje, že [typ zariadenia] spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	[Valmistaja = manufacturer] vakuuttaa täten että [type of equipment = laitteen tyyppimerkintä] tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar [företag] att denna [utrustningstyp] står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.